MANUAL DE CRIMES INFORMÁTICOS

Damásio de Jesus
José Antonio Milagre

Editora Saraiva

SUMÁRIO

A Deus, a Jaline Gilioti e a minha filha Stephanie Milagre.

"Amados, amemo-nos uns aos outros; porque o amor é de Deus;

e qualquer que ama é nascido de Deus e conhece a Deus.

Aquele que não ama não conhece a Deus; porque Deus é amor". 1 João 4:7-8

José Antonio Milagre

À minha neta Marina, doçura de pessoa.

Damásio de Jesus

AGRADECIMENTOS

A Ewerson Guimarães e Filipe Balestra pelas horas dedicadas na reflexão das questões técnicas.

A todos os profissionais de segurança da informação e direito digital do Brasil.

José Antonio Milagre

1.

INTERNET, TECNOLOGIA E O DIREITO

A Internet é rica, e onde há riqueza, existe crime. Segundo Eric Schimidt (NERY, BITTENCOURT, AZAMBUJA, 2013, p. 1), “a internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos”[1]. É inegável que a globalização proporcionou profundas modificações na sociedade contemporânea. Este processo, iniciado na segunda metade do século XX, é fator no rompimento de barreiras econômicas entre países, integrando sociedades. Vive-se em uma aldeia global, expressão criada por Herbert Marshall McLuhan (1964). Da globalização, surge a sociedade do conhecimento, ou a nova economia, ou, ainda, a sociedade da informação. Vivemos uma economia global e informacional.

A este fato soma-se o atual estágio da sociedade, considerada da “informação”. No atual modelo social, a informação é riqueza, poder e o motor para o desenvolvimento e bem-estar social. Tal sociedade da informação é caracterizada pela criação de diversos meios e ferramentas comunicativas de modo a aprimorar seu padrão de vida. Vivemos um dilúvio informacional (LEVY, 1999).

É preciso que se diga que a sociedade não é uma pedra, estática, mas um organismo de mudanças, em constante transformação. A tecnologia é um dos fatores que motivam as principais mutações sociais nesta era, chegando a ditar comportamentos e a criar costumes.

É inerente a esta sociedade que o acesso livre às tecnologias e à rede seja um direito de todos os cidadãos. Mais do que isso, garantias e liberdades constitucionais passam a ser consideradas e refletidas à luz dos impactos que as novas tecnologia trazem no dia a dia. Nas escolas, no trabalho ou nas relações pessoais, estar *online* é realidade, não no mero contexto de estar conectado, mas no

sentido de estar incluído digitalmente, algo além do tradicional ler e escrever, diga-se, ser um ser social digital, estar “em rede”. Para muitos, vivemos em uma sociedade absolutamente discriminatória. Entre os riscos, a substituição da escola, onde jovens amoldados a novas tecnologias poderiam entender que elas, “por si sós”, podem lhes proporcionar todo o conhecimento necessário para viver. Para Nicholas Carr (apud GERSCHENFELD, 2010, p. 2), a Internet está mudando a nossa forma de pensar. Estamos terceirizando nossa memória e nossa identidade.

Por debaixo do capô desta sociedade, uma infraestrutura de meios comunicativos que interliga os continentes. Na sociedade da informação, muitas vezes passa despercebido o aparato estrutural destinado a suportar as comunicações e, por que não dizer, suportar as relações sociais, que se passam no mundo dos *bits*. Vivemos uma sociedade em que nos comunicamos muito, sem saber como tal comunicação é possível, como, quando e por onde. A dominância informacional é flagrante, embora nem todos reconheçam. E informação é poder.

A convergência tecnológica, a dinâmica industrial e a queda dos preços dos equipamentos, aliados ao vertiginoso crescimento da Internet, são as molas propulsoras das recentes transformações sociais locais. O Brasil ultrapassa pela primeira vez 100 milhões de usuários de Internet[2]. A evolução foi rápida, eis que duas décadas atrás utilizávamos redes Fidonet, conectando-se com pessoas através de BBSs (*Bulleting Board Systems*) e *modems* que nos permitiam o acesso discado, muitas vezes em não mais que 56 kbp (*kilobytes* por segundo).

A estrutura deixada pelas pesquisas e pelos militares hoje é utilizada por cidadãos em todo o mundo. A ARPANET (Advanced Research Projects Agency Network), a primeira rede operacional de computadores à base de comutação de pacotes, tornou-se a base de uma rede de comunicação global de milhares de redes de computadores. Deste modo, a *sociedade da informação* é inevitável. Todos os países caminham para ela. Nesta sociedade, busca-se conhecimento sobre como se conseguir mais conhecimento. Nela, porém, a falta de regras e claros princípios pode comprometer a tentativa de um país se beneficiar de suas características e tecnologias associadas. Vivenciamos uma

profunda lentidão nas negociações e acordos internacionais no campo das novas tecnologias, o que, sabe-se, gera barreiras entre países, considerando as regulamentações internas que são criadas. Normas que protejam o cidadão em face da automação e dos riscos do uso indevido das novas tecnologias são consideradas necessárias. O arcabouço legal sempre foi uma das barreiras à perfeita fruição da simbiose entre pessoas e empresas, por meio da tecnologia da informação. Sem legislação, estabelece-se a insegurança jurídica em questões de tecnologia.

Um dos fundadores da Internet, Tim Berners-Lee (junho, 2006), contrariando o que muitos imaginariam, chegou a afirmar que "foi sugerido que não necessitamos de legislação sobre a Internet, pois até hoje não temos legislação e ela não teria feito falta". E continua: "... é bobagem, porque tínhamos liberdade no passado, mas as ameaças explícitas e reais a esta liberdade surgiram apenas recentemente"[3].

E a sociedade da informação (ou para muitos, pós-industrial) tem, sim, seus riscos. Pode ser chamada de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser mitigados. E um deles está associado à criminalidade digital. Ao considerarmos que nem todo o cidadão decidiu ingressar mas lançado foi no universo digital, constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos, os *crackers* (repise-se, e não *hackers* – estes, pesquisadores de segurança da informação), que exploram as intimidades dos sistemas e também dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos. Um mundo onde os *crackers* são os mais fortes. A tecnologia revela um poder imenso a programadores, profissionais de segurança e a qualquer um que conheça a fundo suas intimidades. E o grande problema é o uso deste poder para más finalidades, sobretudo em um país onde educação digital (que não se confunde com aulas de informática) passa longe das escolas.

Não podemos aceitar que na sociedade da informação vigore a lei de talião[4], autotutela ou a lei do mais forte, mas é sabido que o Direito deve prevalecer, fazendo valer a justiça nos conflitos entre cidadãos desta sociedade digital. Faz-se preciso o mínimo de controle para fazer frente àquele que

realiza uma conduta antissocial cibernética. Ser internauta não é delito, assim como ser cidadão não é infração criminal, mas ambos, internauta ou cidadão, podem praticar, sim, infrações. É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser responsabilizado por fato que a lei desconsidera como de relevância penal.

Logo, o Direito, como ciência humana, não pode ficar para trás. Leis que estabeleçam os direitos dos usuários da Internet e deveres dos prestadores são fundamentais para que o Judiciário possa fazer frente a violações e riscos inerentes a sociedade da informação, e, sobretudo, de modo a evitar decisões contraditórias e injustiças diante de casos concretos. Marcos civis regulatórios da Internet são apontados como fatores para o fortalecimento de uma sociedade na era da informação, em suas múltiplas dimensões, social, cultural e econômica, e vêm sendo estudados em todo o mundo (CARVALHO, 2014).

No Brasil, preferiu-se o caminho contrário. Adotando-se primeiramente a legislação criminal (que deveria ser a *ultima ratio*), de modo a punir condutas praticadas por intermédio ou contra sistemas informáticos. Os direitos dos usuários vieram depois com a Lei n. 12.965/2014, denominada “Marco Civil da Internet”. Uma sociedade que não está preparada para entender o que pode caracterizar ou não um crime informático, mas que a despeito já o tipifica, inconsequentemente.

Após quase 15 (quinze) anos de discussões, são promulgadas as Leis n. 12.735/2012 e n. 12.737/2012, esta considerada a Lei de Crimes Informáticos. Passa o direito brasileiro a fazer frente a algumas condutas ilícitas na seara da informática. Como veremos na presente obra, muitas dificuldades virão da interpretação dessa lei. É preciso esclarecer o que está contido no contexto da legislação, quais condutas, práticas, técnicas poderão ser repreendidas pelo Judiciário.

Inúmeras já são as publicações sobre crimes cibernéticos no Brasil, porém muitas são artigos publicados na rede e que consideram a Legislação Projetada ou mesmo buscam adaptações para a aplicação do sistema penal vigente. Neste trabalho, consideram-se as leis recentemente ingressadas

no ordenamento jurídico brasileiro, n. 12.735 e n. 12.737, ambas de 2012, e seus impactos na sociedade da informação, com um olhar sob a ótica da segurança da informação. Assim, o presente livro, visando considerar as leis em vigor e que regulamentam crimes informáticos no Brasil, apresenta um panorama completo e geral sobre as normas, à luz de condutas técnicas comumente praticadas e posturas de segurança da informação, oferecendo embasamento doutrinário e técnico para operadores do Direito e Tecnologia da Informação. No geral, revisita institutos do Direito Penal informático, sempre correlacionando condutas informáticas a padrões jurídicos propostos ou estabelecidos.

Embora sejam leis com poucos artigos, são inúmeros os pontos obscuros e omissos trazidos pela legislação embrionária, e que deverão ser considerados pelos advogados, promotores, juízes, aplicadores do Direito, profissionais de Tecnologia da Informação, profissionais de segurança da informação e cidadãos. Neste cenário, a presente obra, lançando as primeiras interpretações e longe de ser palavra final sobre o tema, vem a contribuir como um dos marcos referenciais teóricos para a correta aplicação das leis vigentes, fornecendo reflexões, dúvidas, elementos e embasamentos técnicos para que se possam distinguir, das inúmeras condutas praticáveis no ciberespaço, quais podem ser enquadradas ou não, para que efetivamente possam as leis atender ao seu mister, e não, ao contrário, ser utilizadas para a persecução de inocentes ou enquadramentos forçosos e absurdos.

Propõe-se, assim, um estudo detalhado das Leis n. 12.735/2012 e n. 12.737/2012, apresentando interpretações minuciosas de todos os seus artigos.

Nas próximas páginas, o leitor conhecerá em detalhes as leis que tratam de crimes informáticos no Brasil. Mais que isso, conhecerá a evolução histórica, conceitos e características que regem o estudo do Direito Penal Informático.

2.

CRIMES INFORMÁTICOS

2.1. Evolução histórica

Em 1820, Joseph-Marie Jacquard[5] produziu a máquina de tear, na França. Seu invento, automatizado, possibilitava a repetição de uma série de passos, antes executados por humanos, para produção de tecidos especiais. A automação incomodou e resultou em medo dentre os funcionários de Jacquard. Seus empregos tradicionais, do qual tiravam sua subsistência, estavam sob ameaça. Foi quando cometeram atos de sabotagem para desencorajar Jacquard no uso da então nova tecnologia.

Em 1939, Alan Turing é recrutado pelo Serviço de Inteligência Americano para descobrir o segredo das máquinas codificadoras eletromagnéticas. Já se estudava a quebra de técnicas e códigos para se ocultar ou proteger a informação.

A era dos computadores modernos se inicia com Charles Babbage. Vivemos o romantismo dos números e a busca por uma linguagem universal. Por que não o "0" e o "1"? No mundo, a literatura internacional indica que os crimes informáticos tiveram seu início na década de 1960, onde identificamos as primeiras referências sobre o tema, em sua maioria delitos de alteração, cópia e sabotagem de sistemas computacionais. Na década de 1970, já era possível ouvir menções ao termo *hacker*. Daniel Bell (1979) fez menção ao termo "sociedade da informação" no final dos anos 1970. "A informação é necessária para organizar e fazer funcionar tudo, desde a célula até a General Motors" (BELL, 1979, p. 169). Em 1970, a IBM já realizava propagandas em torno da "sociedade da informação".

A doutrina diverge acerca do primeiro delito informático cometido. Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (*Massachusetts Institute of Technology*), no ano de

1964, onde um aluno de 18 anos teria cometido um ato classificado com cibercrime, tendo sido advertido pelos superiores.

Outros ainda referenciam o primeiro caso de que se tem notícia sobre *hacking* no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática.

Segundo Schjolberg[6] (2008, p. 1), muitas pessoas estiveram engajadas no combate ao crime eletrônico no passado. Muitos indicam o americano Donn. B. Parker como um dos primeiros pesquisadores sobre cibercrime, com sua pesquisa, quando consultor de segurança para a *Stanford Research Institute*. Ele fora o autor do manual para autoridades de aplicação de leis denominado *Computer Crime – Criminal Justice Resource Manual*, desenvolvido em 1979 e que virou uma "enciclopédia" também para autoridades de fora dos Estados Unidos. Outros autores com grande contribuição na seara são August Bequai e Jay Bloombecker.

No âmbito da Europa, o primeiro estudo acadêmico sobre crime eletrônico foi apresentado por Ulrich Sieber (*Computer criminalitatund strafrecht*).

A primeira iniciativa internacional sobre cibercrime foi a Conferência sobre Aspectos Criminológicos do Crime Econômico, ocorrida no âmbito do Conselho da Europa, em 1976, em Estrasburgo.

Entretanto, foi nas décadas de 1980 e 1990 que grande parte dos cibercrimes se propagou. Já na década de 1980, John Draper (Capitain Crunch), conhecido por ser o inventor do *phreaking*, usou um apito para produzir o tom de 2.600 Hz, capaz de enganar o sistema telefônico americano. Deste modo, conseguia realizar ligações gratuitamente.

As condutas mais comuns nesta época eram a disseminação de vírus, pornografia infantil, invasão de sistemas e a pirataria, momento em que começa a conscientização para a segurança de sistemas. Na década de 1990 já ouvíamos falar em *netwar* e *hacktivists* e as primeiras iniciativas no sentido

de governos estruturarem unidades de “guerra de informação”.

Robert Morris foi o responsável por criar um dos primeiros vírus de computador no mundo, que prejudicou 6 mil computadores em 1988. Foi também o primeiro *hacker* a ser condenado pela então nova *Computer Fraud Act* norte-americana. Em 1990, Kevin Mitnick invadiu a rede de computadores das operadoras de telefonia e provedores de Internet dos Estados Unidos. Foi preso em 1995 e ficou cinco anos detido. Ainda em 1990, Kevin Poulsen interceptou as ligações a uma emissora de rádio na Califórnia e por ser o 102º ouvinte, ganhou um Porsche. Foi preso por quatro anos e hoje é diretor do *site* Security Focus. Nunca mais paramos de conhecer novos casos de *hacking* no mundo.

No Brasil temos notícias dos primeiros crimes de *phishing scam* bancário (pescaria de senhas) em 1999[7]. Igualmente, outro caso célebre foi o de um empresário e ex-controlador de uma rede de varejo, acusado à época (1999) de ter enviado, de Londres, *e-mails* para o mercado financeiro com informações falsas alardeando o risco de quebra de um banco[8]. Muito se debateu, a partir de então, sobre os problemas envolvendo a investigação de crimes informáticos, que poderiam ser praticados em qualquer localidade do mundo. Mais que isso, começou-se a refletir sobre a necessidade de leis que tratassem de crimes informáticos.

Ao tratarmos do primeiro crime informático de ameaça, têm-se relatos, no ano de 1997, de uma jornalista que passou a receber *e-mails* de cunho erótico e sexual juntamente com ameaças a sua integridade física, sendo que a polícia descobriu a autoria das mensagens, tendo o autor sido obrigado a ministrar cursos para a Academia de Polícia Civil (DULLIUS, HIPPLER e FRANCO, 2012, p. 3). No mesmo ano, em novembro, a Justiça de Belo Horizonte tirava da Internet páginas com fotografias de crianças em sexo explícito, sendo que o responsável tinha apenas 15 anos de idade.

Em 1998, em julgado que se tornou histórico, no HC 76.689/PB, relatado pelo Ministro Sepúlveda Pertence, o Supremo Tribunal Federal já enfrentava um caso envolvendo pornografia infantil nas antigas BBS (*Bulleting Board System/Internet*). À época, poderia alguém já imaginar que haveria

necessidade de lei específica para responder a tais delitos. Mas não! O Ministro deu aula ao explicar que nem todos os delitos cibernéticos necessitavam de nova tipificação, eis que em muitos a tecnologia era só um novo meio utilizado para concretização de delitos conhecidos. Vejamos:

"'Crime de Computador': publicação de cena de sexo infantojuvenil (ECA, art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores. Tipicidade. Prova pericial necessária à demonstração da autoria: HC deferido em parte.

1. O tipo cogitado – na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.

2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial".

De fato, como já afirmava em 1996 Ivan Lira de Carvalho, "sendo perguntado, por exemplo, se a Internet é um meio novo de execuções de crimes 'velhos' ou é, por si mesma, uma geradora de novos delitos, terei o atrevimento de dizer que as duas partes da pergunta se completam para a resposta: há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela 'net', delitos já de muito tempo conhecidos da sociedade, só que agora

perpetrados com o requinte do *bit*. Óbvio é que a lei deve acompanhar as inovações criadas e experimentadas pela sociedade. Mas, como na maioria dos sistemas jurídicos que têm a lei como fonte principal (é o caso brasileiro), o processo legislativo é bem mais lento do que os avanços tecnológicos e as consequências destes. No entanto, nem por isso os operadores jurídicos devem cruzar os braços, ficando no aguardo de providências legislativas compatíveis com a modernidade das técnicas criminosas. Se é possível o encaixe da conduta antissocial a um dispositivo legal em vigor, não deve o aplicador do Direito quedar-se em omissão"[9].

Em outubro de 2000 o ex-Prefeito Paulo Maluf se tornaria o primeiro político brasileiro vítima de sabotagem digital nas eleições. Em novembro de 2002 o Brasil ganharia o título de maior "exportador" de criminalidade via Internet. A primeira condenação de um pirata virtual, no Brasil, viria apenas em janeiro de 2004, com a condenação de um jovem de 19 anos a seis anos e quatro meses de prisão por aplicar golpes pela Internet no Brasil e nos Estados Unidos[10].

Deste modo, verifica-se que condutas informáticas danosas são conhecidas há pelo menos quatro décadas no mundo e há quase vinte anos no Brasil, buscando o Direito acompanhar e proteger os que são lesados, de um lado, aplicando a legislação vigente, e, de outro, concebendo tipos penais específicos, considerando a impossibilidade de "analogia *in malam partem*" e os novos bens jurídicos surgidos no âmbito da sociedade da informação.

2.2. Dados sobre crimes informáticos no Brasil e no mundo

O Brasil passou a tratar e se preocupar com o tema nas últimas duas décadas. Hoje, o país é o quarto do mundo com o maior número de ameaças virtuais[11].

Pesquisas sempre revelaram que o Brasil está na rota dos crimes cibernéticos. De acordo com a Polícia Federal, em notícia do ano de 2004, de cada dez *hackers* ativos no mundo, oito vivem no Brasil[12]. Não bastasse, segundo o órgão, à época, dois terços dos responsáveis pela criação de páginas de pedofilia na Internet, detectadas por investigações policiais brasileiras e no exterior,

teriam origem brasileira[13]. A mesma Polícia Federal já afirmou que o crime informático gera mais dinheiro que o narcotráfico[14]. Dados do CNB – Colégio Notarial do Brasil – indicam que o número de crimes virtuais no país aumentou 70% entre 2012 e 2013 (KURTZ, 2014, p. 1).

A *web* permite que os criminosos tenham acesso a muitas vítimas, logo, estamos a falar da escalabilidade do cibercrime. Além disso, técnicas são utilizadas e *crackers* recrutados para ocultar atividades de criminosos. As invasões às estruturas críticas dos países crescem a ritmo inimaginável e no Brasil não é diferente.

Os crimes cibernéticos atingiam em 2011, diariamente, 77 mil brasileiros, com um prejuízo anual de R$ 104 bilhões, segundo levantamento da Norton[15] Mas os números devem ser vistos com cautela, pois são muito variáveis de empresa para empresa.

Já de acordo com a Symantec, o crime cibernético teria gerado prejuízo de R$ 15,9 bilhões entre 2011 e 2012[16], e o valor indicado pelo estudo seria dez vezes maior do que o apontado pela Federação Brasileira de Bancos (FEBRABAN), que apontava R$ 1,5 bilhão, deste, R$ 900 milhões em fraudes bancárias, incluindo cartões de débito e crédito.

Para 2012, segundo dados da F-Secure, o Brasil anualmente registraria prejuízo da ordem de R$ 40 bilhões[17].

Enquanto no Brasil pouco se faz em estrutura investigativa, nos Estados Unidos o FBI convoca especialistas de segurança para o que anuncia ser uma “Guerra Cibernética”[18], eis que o crime informático estaria se tornando uma ameaça maior que o próprio terrorismo. Crime informático não é só questão de segurança pública, mas de defesa nacional.

Em acórdão do STF, em 2005, o Ministro Gilmar Mendes chegou a reconhecer a existência do cibercrime organizado no Brasil[19]. Uma pesquisa realizada pelo Ponemon, denominada “Percepções sobre segurança na rede”, indica que, no mundo, fraudes digitais, roubo de propriedade intelectual e danos às redes corporativas já geraram um prejuízo de U$$ 1 trilhão em apenas um ano. Pela pesquisa, o Brasil é o segundo maior país em número de crimes cibernéticos[20]. Por outro lado,

investe-se muito aquém do necessário (e disponível) em defesa cibernética[21].

Quando falamos em macrocriminalidade, o Brasil destaca-se como quarto principal alvo dos *crackers* em ataques de *phishing* (pescaria de senhas) no mundo, figurando entre os cinco países que mais tiveram empresas hackeadas[22]. Algo em torno de 38 milhões de usuários lesados[23]. Já a média mensal de crimes virtuais contra crianças cresceu 57% em 2012[24].

Em 2013, o país perderia U$$ 8 bilhões com ataques de *crackers*, roubos de senhas, clonagens de cartões, pirataria virtual, além de espionagem governamental e industrial, entre outros crimes cibernéticos[25]. Crimes de informática custaram U$$ 500 bilhões para a economia mundial em 2013[26].

A sociabilidade do brasileiro pode ser identificada como favorecedora dos crimes digitais, sobretudo numa era envolvendo *apps* falsos, que muitas vezes não são checados por seus usuários antes de serem instalados. E o risco aumenta, pois cibercriminosos passam a focar na Internet das Coisas, como TVs, geladeiras e carros conectados. Cinquenta e sete por cento dos usuários de *smartphone* brasileiros foram vítimas de crime virtual móvel (GONZAGA, 2013).

Segundo Peter Armstrong (FENSEG, 2015), os ataques cibernéticos aumentaram 48% em 2014, segundo estudo “Managing cyber risks in an interconnected world”, da PWC. Acrescenta o levantamento que o número de incidentes cibernéticos detectados subiu para 42,8 milhões em relação a 2013 (o equivalente a 117.339 novos ataques todos os dias).

Tais números, meramente exemplificativos, mostram quão grande é a necessidade de esforços para que o Direito Penal possa proteger os cidadãos dos riscos da sociedade da informação.

3.

LEGISLANDO SOBRE CRIMES INFORMÁTICOS

O Brasil adota o sistema da reserva legal. Não há crime, sem lei anterior que o defina. Especialmente quando tratamos de tecnologia da informação, a técnica para criar leis deve ser outra. Isto porque o legislador deve ter o cuidado para que não conceba uma ordenação jurídica natimorta, que ingressa no arcabouço legislativo de modo ultrapassado.

Neste contexto, há muito tempo se cobrava uma legislação no Brasil que cuidasse de crimes eletrônicos. Tal mora pode ser atribuída também ao péssimo modo de se legislar sobre o tema adotado no Brasil que, por vezes, tentou condenar técnicas informáticas (ao invés de condutas praticadas por diversas técnicas), técnicas estas que são mutantes, nascem e morrem a qualquer momento, de acordo com a evolução dos sistemas, novas vulnerabilidades e plataformas tecnológicas. Para isso apresentamos uma proposta de sistematização e que deve ser considerada quando se legisla sobre crimes informáticos. Nominamos a proposta de TCC – Técnica, Comportamento e Crime. A proposta é detalhada na sequência.

3.1. A teoria TCC: Técnica, Comportamento e Crime

Para que se possa conceber uma legislação minimamente eficiente, eficaz e que não precise ser complementada com o tempo, bem como para que se possa compreender o crime digital, importante se faz sistematizá-lo da seguinte forma:

• *Técnica*: método, procedimento, *software* ou processo informático utilizado e que pode caracterizar um comportamento. Uma técnica pode ser executada manualmente ou por meio de subtécnicas, métodos automatizados ou ferramentas. A exemplo, um agente que obtém acesso a dados

de um repositório pode estar utilizando a técnica de *sql injection*.

• *Comportamento*: uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, por ação ou omissão, em face de redes de computadores, dispositivos informáticos ou sistemas informatizados. No mesmo exemplo citado acima, por meio da técnica *sql injection*, o agente praticou o comportamento "invasão de sistema informático".

• *Crime*: um ou vários comportamentos, que utiliza uma ou mais técnicas, que ofende um ou mais bens ou objetos jurídicos protegidos pelo Direito. Mantendo o mesmo exemplo, a "invasão de sistema informático" pode ser ou não considerada crime, dependendo do país em que é praticada.

Apresentada nossa sistematização, temos o primeiro princípio: Não se legisla sobre técnica! Qualquer tentativa de legislar sobre técnicas e métodos de um ataque resulta em uma legislação por demais específica e pouco eficaz, com rápida obsolescência. Muito menos se legisla sobre vulnerabilidade.

Logo, identifica-se primeiramente um comportamento que possa ser concretizado por uma ou mais técnicas informáticas, que existam ou que venham a ser criadas. Comportamento este que mereça a tutela penal e, neste sentido, se eleva tal comportamento ao *status* de "crime", se realmente corresponder a uma atividade reprovável.

Até mesmo ao se definirem os elementos que fazem parte de um comportamento, deve-se ter cautela em não especificá-los ao extremo a ponto de não poder abranger condutas que "ao lado" sejam ofensivas ao bem jurídico e que não poderão ser enquadradas. Por outro lado, não pode ser um tipo muito aberto, que poderá resvalar em condutas legítimas e triviais.

Por exemplo, a Lei n. 12.737/2012, que será estudada no Capítulo 8, traz uma alteração ao art. 298 do Código Penal, falsificação de documento particular, onde faz prever a equiparação a documento particular o cartão de crédito ou débito. Perceba-se que o documento particular é elemento indispensável ao comportamento reprovável. Tem-se, pois, que sem um "documento particular" se torna impossível realizar a conduta "falsificar".

Ao equiparar o cartão de débito ou crédito ao documento particular, o legislador foi específico ao objeto, porém não resolveu a questão da interpretação envolvendo os inúmeros documentos que hoje não estão sob um suporte material. Logo, alguém que falsifique um documento que está contido em um suporte *token* ou *pendrive*, pelos princípios penais, praticaria fato atípico. Uma limitação do objeto do comportamento. Mais prudente seria, ao legislador, equiparar o documento particular aos documentos, informações e declarações eletrônicas, representadas ou não em suporte material, de qualquer natureza.

Assim, ao se legislar sobre crimes informáticos, não se começa pela análise de uma técnica, tampouco definindo tipos penais, mas analisando condutas incrimináveis que podem ser realizadas por diversas formas (técnicas), e que mereçam a consideração do Direito Penal. Do mesmo modo, uma técnica pode ser integrante de uma ou mais condutas penalmente relevantes. Um "cavalo de troia", por exemplo, pode servir a uma invasão, mas também para permitir o dano ou mesmo o comportamento inesperado de um sistema informático. Por outro lado, nem toda a técnica se enquadra em um comportamento incriminável.

Este pode ser, *data venia*, um dos principais erros de grande parte dos doutrinadores e legisladores sobre o tema: confundirem técnica com conduta. A falta de apoio técnico – especialistas em tecnologia e segurança da informação, em setores legislativos – leva o legislador brasileiro à criação de tipos penais incoerentes.

Vírus de computador não é conduta incriminável, *phishing scam* (dependendo da técnica empregada) pode também não ser, muito menos o *sniffing*. Não raro, entretanto, encontramos livros classificando tais artefatos ou técnicas como condutas incrimináveis, logo, potenciais tipos criminais! Um grande erro.

O vírus, em verdade, está inserido na conduta provocar ou tentar provocar dano a um dispositivo computacional, ou fazê-lo funcionar de forma inesperada, por caracterizar uma sabotagem informática. Não significa dizer que tal conduta só possa ser realizada por meio do vírus! Logo, vírus

não é comportamento ou conduta, mas um artefato capaz de causar dano a um computador. Podemos comprometer um sistema por meio de outros artefatos ou técnicas, *trojan*, *worm*, *hijacking*, dentre outros.

O *phishing scam* (pescaria de senhas), técnica, consiste em apenas uma das formas para que o agente obtenha vantagem ilícita, induzindo alguém em erro (conduta) e proporcionando a entrega ao atacante de informações confidenciais da vítima.

O *sniffing* constitui apenas uma das técnicas possíveis para que o agente realize a conduta de interceptação telemática, que pode ser, por exemplo, por meio de outras técnicas ou conceitos, como *arp poisoning* e *man in the middle.*

Assim, resta claro um equívoco por grande parte da doutrina, um paradigma a ser superado. A perfeita distinção entre técnica, arma do crime (artefato) e comportamento. É fundamental que o operador do Direito reflita, diante de cada técnica, se a mesma efetivamente corresponde a um comportamento incriminável. Igualmente, o operador do Direito digital deve fazer uma análise se o artefato utilizado pode ou não corresponder a uma atividade criminosa. Neste livro, sem pretensão de esgotar o tema, propusemo-nos a fazer este raciocínio. Ao trazer o tipo de "invasão de dispositivo informático", a Lei n. 12.737/2012, objeto deste livro, apresenta uma conduta que poderá ser realizada pelas mais variáveis técnicas possíveis, conhecidas ou que se inventem no futuro, como exploração de um *backdoor, password guessing, brutal force, dictionary attack*, *sql injection,* dentre outros.

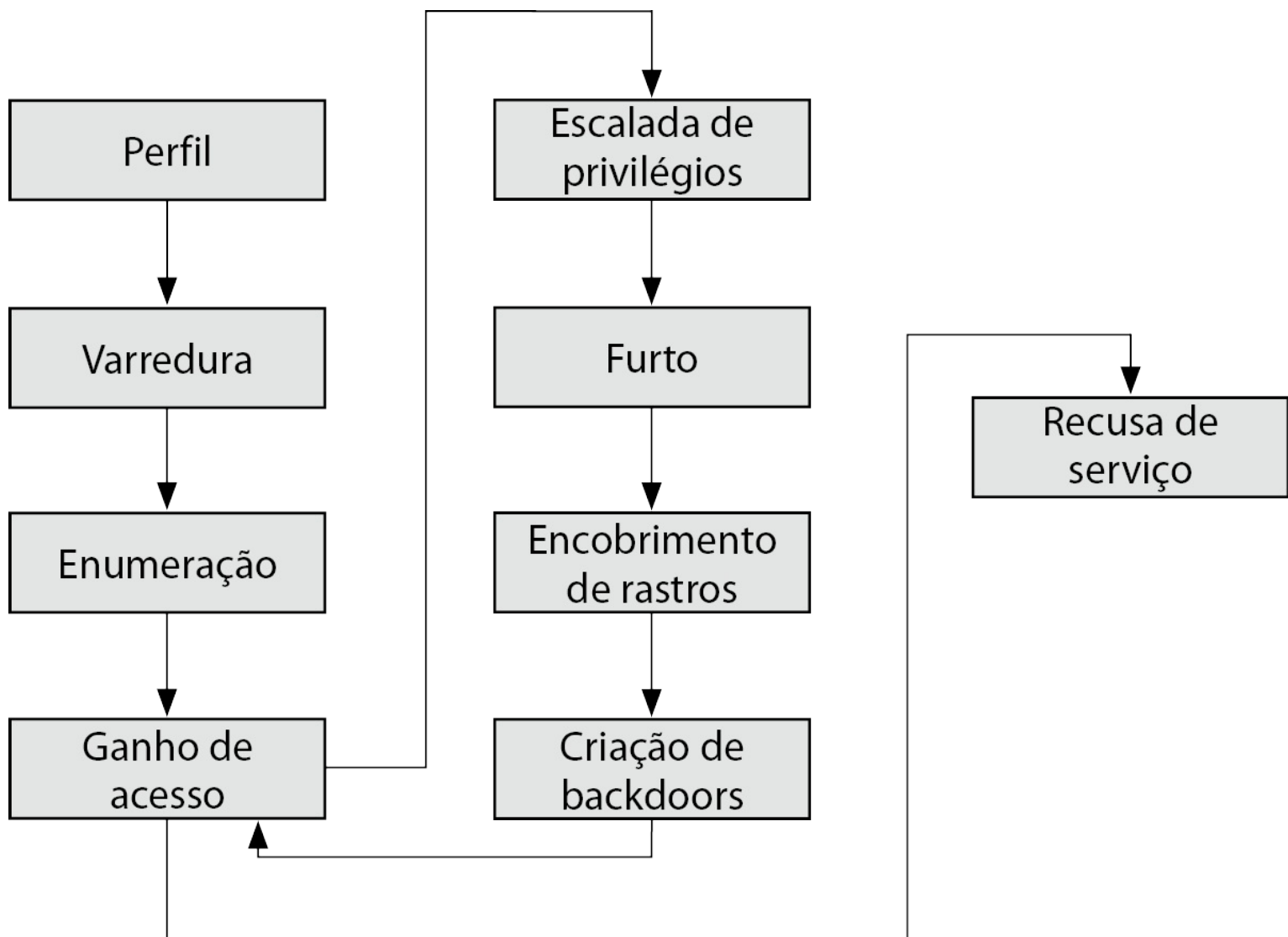
Ao prever o tipo penal de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, o legislador descreveu uma conduta, punível, que pode ser consumada por meio de diversas técnicas, como ataque de negação de serviço (DoS), ataque de negação de serviços distribuídos (DDoS), dentre outras.

Conhecer a técnica é fundamental para o operador do Direito. Não se pode exercer com dignidade a advocacia em direito digital sem conhecer a fundo as técnicas. Não se pode jogar todas as técnicas

na mesma bacia de um suposto comportamento considerado criminoso. Muitas técnicas utilizadas por *crackers* descaracterizam o pretenso tipo penal. Muitas técnicas, ainda, desviam a conduta da descrita no tipo. Muitas condutas protegidas pela tutela penal não abrangem determinadas técnicas. Diga-se, muitas técnicas isoladamente praticadas não representam condutas incriminadoras. Ter tal sensibilidade é fundamental para que se evitem injustiças e para que se faça uma boa defesa em processos envolvendo crimes informáticos. Tanto para defensores como para autoridades, é mister que não se considere a máxima "o que vale é conduta, pouco importando a técnica". Esta é a luta do advogado criminal informático: impedir as arbitrariedades do Estado, desconhecedor da informática e ansioso em penalizar cidadãos, seja como for.

Como exemplo, podemos citar alguém que acessa diretório FTP *(file transfer protocol)* alheio, sem senha, simplesmente listando os arquivos. Embora esteja dentro de sistema informático alheio, obtendo informações, não realizou a conduta invadir, pois a técnica não foi truculenta, forçada, ou, mesmo, não envolveu a quebra de segurança. Alguém que altera parâmetros aceitáveis de uma variável (alterando, por exemplo, o código de um usuário para outro código e exibindo o registro de outra pessoa/usuário), a ser transmitida ao banco de dados (*query*), conseguindo exibir dados de clientes de um serviço, não pratica em tese, *sql injection*, uma das técnicas relacionadas à conduta de acesso indevido. Obteve informação, usou uma técnica, mas não invadiu nada.

Alguém que pratica um farejamento de redes, a chamada fase de *footprinting*, por meio de programa como *nmap, satan,* em busca de vulnerabilidades, por exemplo, não pode ser responsabilizado pela conduta de invasão de dispositivo ou mesmo de atentado contra serviço telemático, pois sabe-se, trata-se de atos preparatórios, onde a conduta não chegou a ser executada.

É preciso ter em mente a anatomia de um ataque cibernético, que, via de regra, segue a seguinte ordem (podendo variar em cenários distintos):

Anatomia de um ataque cibernético

Estes são, via de regra, os principais passos percorridos por um atacante para a invasão de um dispositivo informático. Repetimos: pode-se variar. Em nossa visão, a relevância criminal (art. 154-A do Código Penal) começa a existir na fase "Ganho de acesso", onde efetivamente dá-se início a atos executórios, relacionados à invasão. As fases de "Perfil", "Varredura" e "Enumeração" se enquadrariam em atos preparatórios, não puníveis.

Alguém que acessa dispositivo informático desprotegido, e lá, lista informações confidenciais de clientes, não pode ser enquadrado na conduta de furto, considerando que não existiu a transferência das informações para seu computador. Do mesmo modo, não pode ser enquadrado na conduta envolvendo divulgação de segredo, considerando não ser o destinatário ou detentor da informação que visualizou. A informação continua onde sempre esteve.

Quem faz com que a vítima pratique um *download* de um arquivo de sistema que explora o navegador com técnica *xss-cross-site* não pode ser punido por dano ou por invasão de sistema informático. Da mesma forma, quem desenvolve prova de conceito ou ferramenta para avaliação de redes não merece ser confundido com aquele que desenvolve aplicação para a prática de crimes informáticos. E é possível estabelecer esta distinção.

Um *malware* pode não ser um vírus que cause dano ou capture informações. *Malware* é gênero e significa código malicioso, mas não significa necessariamente um artefato encartado em uma conduta penalmente imputável. Posso ter um *malware* inofensivo ou meramente conceitual. Não podemos, repise-se, colocar tudo na mesma bacia.

A execução de comandos remotos, pelo atacante, operando um *backdoor,* não implica conduta de invasão, pois o atacante pode ser apenas quem "explora" a precitada vulnerabilidade. O *sniffing*[27] (farejamento de dados) de uma rede aberta pode não constituir interceptação[28].

Quem poderá distinguir tais casos são os operadores do Direito, que deverão se atualizar tecnicamente ou, ao menos, reconhecer a deficiência técnica, valendo-se de peritos e assistentes capacitados. Isto porque, como visto, a tendência é que leis sobre crimes informáticos sejam promulgadas sem observância à teoria TCC (Técnica, Comportamento e Crime), gerando insegurança jurídica e risco de interpretações errôneas.

4.

ARTEFATOS, TÉCNICAS OU MÉTODOS PARA A PRÁTICA DE CONDUTAS QUE PODEM SER CONSIDERADAS CRIMES INFORMÁTICOS

Apresentamos, a seguir, de forma básica para a compreensão dos operadores do Direito, os principais artefatos, técnicas ou métodos informáticos, que podem estar associados a um ou mais comportamentos ou ataques considerados relevantes para o Direito Penal. Logicamente, temos muito mais técnicas e armas do que comportamentos, razão pela qual apresentamos as principais ou mais comuns.

4.1. Vírus

Espécie de *malware*. Programa de computador com a capacidade de alterar dados ou sistemas, destruir, alterar arquivos e programas, ou mesmo executar funções inesperadas em um sistema computacional ou dispositivo informatizado. Um vírus capaz de se replicar pela rede recebe o nome de *worm*.

4.2. *Trojan*

Espécie de *malware*. Programa que faria algo além do que parece. "Cavalo de troia" é uma instrução ou código malicioso comumente ocultado em outro *software*, que, instalado, torna um computador ou sistema vulnerável ou mesmo explora vulnerabilidades já existentes. Dependendo do *trojan*, é possível não só acessar um sistema, como se tornar administrador, copiar informações confidenciais. Muito comum o uso de *trojan* em *phishing scam* (*e-mails* maliciosos que falsificam a

identidade visual de instituições e induzem usuários a clicar nestes códigos maliciosos, momento em que são infectados, ou *spear phishing*, que é o *phishing* direcionado, focado em um grupo ou organização específicos). Programas como *binders, joiners* e *packers* podem compactar um *trojan* ou inseri-lo juntamente ao outro programa comum e inofensivo, com um *game* e até mesmo uma apresentação de *slides*.

4.3. *Sniffing*

Técnica consistente em capturar pacotes de dados, transmitidos em redes TCP/IP, onde é possível realizar a interceptação do que é trafegado em uma rede. Normalmente, o tráfego da rede é salvo em arquivos *.pcap* (pacotes) posteriormente interpretados ou codificados em programas específicos, como Xplico, Wireshark ou Tcpxtract. Tráfego de rede não criptografado pode conter dados bancários, senhas e outras informações utilizadas pelo criminoso digital. Também pode ser combinado com outras técnicas como *arp poisoning* (item 4.20).

4.4. *Backdoor*

Código malicioso implantado pelo *cracker* ou *trojan*, que permite o escalonamento de privilégio, a invasão, a tomada do sistema ou o desligamento de mecanismos de segurança. Para alguns especialistas, *backdoor* não é vulnerabilidade, mas um código malicioso que permite acesso facilitado ao sistema ou máquina. Em outras palavras, *backdoor* é um meio não documentado de acessar um sistema, burlando os mecanismos de autenticação. Algumas *backdoors* são inseridas propositalmente por programadores dos sistemas e outras podem ser inseridas por atacantes durante o comprometimento de um sistema, ataque de vírus, *trojan* e *worm*. Normalmente, os atacantes usam *backdoor* para facilitar o acesso futuro a um sistema previamente comprometido.

4.5. *Spyware*

Código ou programa malicioso instalado ou injetado normalmente em aplicativos baixados de fontes duvidosas, que tem a função de coletar informações do usuário de um computador e enviá-las ao destinatário. Informações comumente coletadas são hábitos de consumo, informações de navegação, dentre outros. Alguns permitem o controle da máquina pelo atacante. Também podem estar inseridos dentro de *adwares*, *softwares* não autorizados que exibem propagandas no computador da vítima. Assim como os famosos *cookies*, também se prezam a coletar informações sobre um usuário de um serviço *web*.

4.6. *Keylogging* e *screenlogging*

Técnica para monitorar tudo o que é digitado pela vítima. A captura dos caracteres do teclado é armazenada em arquivo, que é remetido pelo atacante. A evolução desta técnica e dos mecanismos de segurança dos *sites* bancários gera o chamado *screenlogging*, que, ao invés de capturar o conteúdo do teclado, captura *screenshots* (registros) das telas, no escopo de monitorar dados e informações de teclados virtuais. Importante destacar, também, existir *keylogger* físico, onde um adaptador é inserido entre o teclado e o computador. Alguns *keyloggers* físicos possuem mecanismo para enviar tudo via *wireless*, sem necessitar a retirada do mesmo posteriormente para leitura dos dados armazenados.

4.7. *Defacement*

Não é uma técnica (técnica é o que o atacante usou para aplicar o *defacement*), mas consiste na "pichação de *sites*", normalmente usada por *hackers* ou *crackers* em protestos, consiste em remover página principal, inserir mensagens ou alterar conteúdo visual de um sítio na rede mundial de computadores. Quem pratica o *defacement* se vale de uma técnica.

4.8. *Rootkits*

Software que tem a função de corromper a atividade convencional de um sistema operacional, utilitários, bibliotecas, ou arquivos de sistema, fazendo com que ajam de forma diferenciada. Por exemplo, um *rootkit* pode comprometer um programa navegador, que, ao ser executado, também chama uma função que abre uma porta da máquina para ser acessada por um *cracker*. Os *rootkits* também escondem processos e porta abertas que não serão retornados em consultas comuns ao sistema operacional, como, por exemplo, utilizando o comando em Linux *"ps –aux"*.

Tipo de *software* normalmente utilizado por atacantes que têm como objetivo manter um atacante com acesso no alvo. Normalmente ele é composto de um conjunto de *trojans* e *backdoor* para permitir acesso futuro ao atacante e ocultar os processos criados por ele, tais como ocultar a existência de uma *backdoor* ou a execução de um *keylogger* deixado em execução por um atacante no alvo.

4.9. DoS e DDoS

O *Denial of Service* (ou ataque de negação de serviços) consiste em um ataque cuja função é indisponibilizar um serviço informático por sobrecarga. Esse tipo de ataque pode ser realizado através de diversos tipos de técnicas. São exemplos não exaustivos de técnicas:

a) *inundação de pacotes* – consiste no envio de diversos pacotes de rede com o objetivo de congestionar o *link* de conexão da máquina-alvo, impossibilitando usuários legítimos de acessar o sistema devido ao alto tráfego;

b) *problemas de protocolo* – consiste em explorar alguma deficiência do protocolo ou da implementação do protocolo utilizado pelo serviço para comunicação com seus clientes;

c) *problemas de codificação* – consiste em explorar uma vulnerabilidade no *software* que é capaz de fazê-lo parar de funcionar. Exemplo pode ser uma exploração de um Buffer Overflow, que pode causar a parada abrupta do *software*;

d) *ataque de disco* – consiste em encher o dispositivo de armazenamento até que o mesmo não

suporte mais informações, fazendo-o parar de funcionar;

e) *DDoS (Distributed Denial of Service)* – é a utilização de diversas máquinas para a realização de um ataque de negação de serviço. Normalmente é utilizada técnica de inundação de pacotes, pois diversas máquinas possuem capacidade de geração de tráfego muito superior a apenas uma máquina.

Outras técnicas (algumas mais antigas e não mais usuais) são *pingflood*, *floodsmtp*, *floddicmp_echo*, dentre outras. Atualmente temos ataques de Camada 7[29], que não sobrecarregam a Camada 3 (rede) e sim a camada de aplicação.

4.10. *DNS poisoning*

Consiste em alterar os endereços de resolução DNS (*Domain Name System* – Sistema de Nomes de Domínios) de um serviço, direcionando um acesso para um *site* falso ou serviço criado pelo atacante.

4.11. *Brute force*

Também conhecido por força bruta. Técnica para quebra de senhas e acesso a sistemas que consiste em tentar todas as combinações possíveis. Muitas ferramentas hoje disponíveis automatizam o *brute force*.

4.12. Ataque de dicionário

Outra técnica envolvendo quebra de senhas, que consiste testar palavras do dicionário que eventualmente façam parte da composição de uma senha. A mistura de ataques *brute force* com ataques de dicionário para geração de palavras não existentes recebe o nome de *Syllabe*.

4.13. *Rainbow table*

Ataque destinado à quebra de senhas criptografadas, consiste em submeter os *hashs* a uma tabela de *hashs* já calculados para realização de comparações.

4.14. *Scanning*

O escaneamento de portas é uma técnica que consiste em varrer diversos *hosts*, identificando portas abertas, vulnerabilidades e informações, como, por exemplo, o tipo do sistema operacional de um servidor.

Dentre as principais modalidades de *scanning* temos:

a) *Host Scan*: descoberta de máquinas ativas na rede.

b) *Port Scan*: varredura de portas abertas de um *host*.

c) *Vulnerability Scan*: busca por vulnerabilidades em um servidor de acordo com os serviços em execução.

4.15. *Connection back*

Uma técnica ou aplicação (para muitos considerada antiga) capaz de fazer com que a vítima conecte-se diretamente ao atacante, sendo que, de tal conexão, o atacante passa a ter acesso à máquina da vítima.

Normalmente, o atacante é quem tenta se conectar em uma máquina. Porém, muitas vezes um *firewall* local ou de rede pode bloquear essas tentativas ou, mesmo, a máquina não está acessível diretamente na Internet ou o seu endereço IP é desconhecido. *Connection back* é uma técnica que consiste em fazer a máquina da vítima conectar-se ao computador do atacante, o que muitas vezes contorna os problemas descritos acima.

4.16. *SQL injection*

Técnica consistente em alterar parâmetros ou instruções que são executadas sobre uma ou mais tabelas de um banco de dados, por meio da linguagem SQL *(Structured Query Language),* permitindo o acesso indevido, alteração, inclusão ou destruição de informações.

4.17. *Buffer overflow*

Buffer overflow é um tipo de vulnerabilidade e ocorre quando uma variável de um programa recebe mais informações do que ela foi desenhada inicialmente para suportar e o desenvolvedor do sistema não criou nenhum tipo de checagem para evitar que isso ocorra. Os resultados podem ir além de uma simples tecla de erro e interrupção do programa em execução, causando uma negação de serviço e até mesmo a execução de códigos arbitrários no computador que possui o programa vulnerável, através da modificação do fluxo de execução de um programa.

4.18. *Botnets*

Bots são sistemas instalados por criminosos digitais em estações servidoras e que respondem a comandos destes, realizando inúmeras funções. Via de regra, uma máquina se torna um "zumbi" e é utilizada pelo criminoso *handler* para ataques e prática de outros crimes digitais, dificultando a apuração de autoria. *Botnet* em si é uma rede de computadores compostas por vários *bots*, que estão prontos para receber comandos.

4.19. *Session hijacking*

O denominado sequestro de sessão é o procedimento onde o invasor descobre uma conexão TCP ativa entre duas máquinas, assumindo o controle. *Session hijacking* de conexão TCP, nos dias de hoje, quase não existe. Atualmente, fala-se em *session hijacking* de uma aplicação *web,* que consiste em capturar o número/*token* de sessão e utilizá-lo para acessar a aplicação.

4.20. *Arp poisoning*

Placas Ethernet efetuam uma solicitação ARP para que o sistema informe qual MAC Address (endereço físico de um computador) está vinculado a determinado IP. A técnica do envenenamento da tabela ARP consiste justamente em fazer com que outro MAC apareça como responsável pelo IP, normalmente o MAC da máquina do atacante. Isso faz com que a vítima envie os pacotes para a máquina do atacante ao invés da máquina original. Dentre as principais ferramentas para este ataque temos o Dsniff, Cain, Ettercap e Hunt.

4.21. Exploração do Kernel

O Kernel é o núcleo de sistemas operacionais. Método muito sofisticado e de difícil detecção. Com a subversão do Kernel, o criminoso digital pode se tornar invisível a programas de segurança da informação, sistema de detecção de intrusos e outros mecanismos.

4.22. *Watering hole attack*

Atualmente, se o invasor tem dificuldade para invadir empresas maiores e com mais investimentos em segurança da informação, ele tentará invadir sistemas menores de parceiros da empresa-alvo ou mesmo sistemas que funcionários da empresa-alvo acessam. Com esta exploração, usa-se uma maquina pivô, normalmente mais vulnerável, para se acessar um ambiente informático e acessar o servidor ou máquina do alvo, que de certo modo interagia com o pivô infectado.

5.

CONDUTAS INFORMÁTICAS QUE PODEM CARACTERIZAR CRIME

No capítulo anterior verificamos uma série de técnicas e artefatos que podem representar condutas informáticas. Neste capítulo apresentamos as principais condutas, que podem se evidenciar por meio de uma ou mais técnicas ou artefatos e revelamos se a legislação brasileira faz ou não frente a tais condutas.

Comportamentos informáticos (com o auxílio de *hardware* ou *software*) são ou deveriam ser objeto de legislação penal e não as técnicas ou armas usadas pelo comportamento. Como dito, devemos sim é analisar se as técnicas empregadas estão ou não contidas no comportamento. No Brasil, há mais de 12 anos, busca-se desenfreadamente legislar sobre crimes digitais, de forma errônea e inconsequente.

Os primeiros legisladores buscavam punir técnicas ou armas, como visto, um erro, pois as técnicas, artefatos e as armas cibernéticas se modificam. Posteriormente, passaram a definir dezenas de comportamentos, uns até mesmo que coincidiam com outros, gerando uma redundância criminal.

Em um terceiro estágio, onde fora possível a aprovação das Leis de Crimes Informáticos, objeto do presente livro (Leis n. 12.735/2012 e n. 12.737/2012), chegou-se ao acordo de dar relevância penal apenas a comportamentos considerados intoleráveis ou recorrentes na sociedade.

Comportamentos (ou condutas) são relacionados a potenciais crimes próprios, onde a informática é o bem jurídico agredido. Logicamente, não enumeramos aqui os comportamentos que ofendem outros bens jurídicos, e que podem ser realizados por intermédio da informática, como, por exemplo, encartados nos delitos de pornografia infantil, contrafação, pirataria de *software*, a ameaça, a injúria, dentre outros. Para estes, o Código Penal é suficientemente claro.

A seguir, os principais comportamentos que merecem uma relevância ou a análise do Direito Penal

Informático. Importa dizer que as condutas poderão ou não ser consideradas crimes, o que irá variar de acordo com a maturidade legislativa em matéria informática de um país.

5.1. Acesso ilegítimo

Trata-se do acesso sem autorização, não necessariamente com a violação de medidas de segurança (invasão). Comumente, dá-se em um sistema informático que pode ser conceituado como um dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais deles desenvolve o tratamento automatizado de dados. Para se legislar sobre acesso indevido é importante considerar que as convenções internacionais estabelecem que seja necessário indicar que tal acesso deve ter intenção ilegítima. No Brasil, para parte da doutrina o acesso ilegítimo ganha *status* de tipo penal, com a Lei n. 12.737/2012. Já para outros autores, o Brasil pune com o art. 154-A do Código Penal somente a invasão (acesso ilegítimo forçado, com rompimento de obstáculo).

5.2. Interceptação ilegítima

É a conduta relacionada ao uso de meios técnicos, em transmissões não públicas, para interceptação e captura de dados e informações. Tal conduta pode ser punida, no Brasil, nos termos do art. 10 da Lei n. 9.276/96.

5.3. Interferência de dados (dano informático)

É o ato intencional e ilegítimo, realizado por um ou mais agentes, no escopo de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. Diz respeito em verdade ao dano informático. No Brasil, embora tenha sido previsto no Projeto de Lei n. 84/99, na publicação da Lei n. 12.735/2012, o “dano informático” foi suprimido. Logo, se da invasão decorre o dano, temos agora a incidência do art. 154-B do Código Penal, nos termos da nova Lei n. 12.737/2012. Se, porém, o agente não invade,

mas apenas causa o dano informático, ainda nos valemos do Código Penal de 1940, na subsunção ao art. 163 (crime de dano).

5.4. Interferência em sistemas

Está relacionada à conduta daquele que, dolosamente, causa obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, por meio da introdução, transmissão, danificação, eliminação, deterioração ou supressão de dados informáticos. No Brasil, não temos um tipo que tutele os bens jurídicos de todas as condutas acima narradas. Com a edição da Lei n. 12.737/2012, temos a tipificação do delito de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, que, em verdade, cobre parte das condutas acima descritas.

5.5. Uso abusivo de dispositivos

Diz respeito à conduta de produzir, vender, obter, utilizar, importar ou distribuir dispositivo ou programa informático concebido para fins da prática de outras condutas criminosas ou mesmo senhas, códigos de acesso e dados informáticos que permitam o acesso indevido a sistemas. Com a publicação da Lei n. 12.737/2012, temos parte destas condutas cobertas pelo art. 154-A do Código Penal, onde a lei pune não só o invasor, mas o que desenvolve e distribui ferramentas com esta finalidade. No art. 325 do Código Penal, que trata da violação de sigilo funcional, temos a pena de detenção de seis meses a dois anos e multa para o agente que permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública.

5.6. Falsidade ou fraude informática

É a introdução, alteração, eliminação ou supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que sejam considerados ou utilizados legalmente como se fossem autênticos. No Brasil, não temos um tipo específico para tutelar esta conduta em casos de bancos de dados privados (podendo se cogitar do delito de falsidade ideológica – art. 299 do Código Penal). Já no âmbito dos crimes praticados por funcionário público contra a Administração Pública, temos o art. 313-A do Código Penal, inserido pela Lei n. 9.983/2000, que assim define, cominando pena de dois a doze anos de reclusão e multa: inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida, para si ou para outrem, ou para causar dano.

Da mesma forma, o art. 313-B do Código Penal pune, com pena de detenção de três meses a dois anos, a conduta de modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. Já para o particular, que acessa bancos de dados da Administração Pública de forma indevida, tem-se a punição prevista no inciso II do § 1º do art. 325 do Código Penal.

5.7. Burla informática

É ato intencional e ilegítimo, do qual origine dano, mediante introdução, alteração, eliminação ou supressão de dados informáticos, ou qualquer intervenção no sistema informático com a intenção de benefício econômico. É também conhecida como *sabotagem informática*. Não se tem um único tipo claro, no ordenamento jurídico brasileiro, para fazer frente a tal conduta.

5.8. Furto de dados ou vazamento de informações

Consiste em copiar ou mover, indevidamente, informações protegidas ou confidenciais. Para punir a cópia indevida, muitas autoridades utilizaram da analogia *in malam partem* para classificar o ato

como “contrafação”, “furto de dados”, outros partiram para a “interceptação telemática”, prevista na Lei n. 9.276/96. Outros autores ainda enquadravam a cópia indevida na concorrência desleal, crime previsto no art. 195 da Lei n. 9.279/96. Em verdade, não existe um tipo específico para esta conduta. Já para o vazamento de informações tem-se forçosamente utilizado o tipo do art. 153 do Código Penal (divulgação de segredo), sobretudo quando a divulgação se dá em relação a informações sigilosas, contidas ou não nos sistemas de bancos de dados da Administração Pública. A Lei n. 12.737/2012 trata essa circunstância como uma qualificadora do crime de “invasão de dispositivo informático”, com pena de reclusão de seis meses a dois anos e multa, se a conduta não constitui crime mais grave, quando da invasão ocorrer a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.

Importa dizer que o ex-empregado que acessa seu *e-mail* ainda ativo, e lá recupera informações, não poderá ser responsabilizado por acesso indevido (art. 154-A do Código Penal). Poderá, analisando-se o caso, responder pelas condutas que sucederem o acesso, como uma possível conduta afeta à concorrência desleal. Trata-se, pois, de uma negligência da empresa, que não removeu as credenciais do colaborador quando do seu desligamento. Neste sentido a norma ISO 27001/2006, que institui técnicas de segurança (Sistema de Gestão de Segurança da Informação), *vide* seu objetivo de controle de número A.8.3, cujo propósito é assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de modo ordenado.

Estabelece ainda o controle A.8.3.3 da precitada norma que “os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades”.

5.9. Pichação informática ou *defacement*

Conduta daquele que indevidamente altera *layout* de páginas *web*, *sites* e *intranets*, em alguns casos promovendo a pichação por meio de inclusão de textos ou figuras indevidas no código do *site* (html) ou mesmo no banco de dados (onde também temos uma conduta de acesso indevido). Na grande maioria das vezes (mas nem sempre – como em alguns casos de *code injection*) a pichação pressupõe uma invasão. Logo, desde 2013, punível nos termos do art. 154-A do Código Penal. Para parte da doutrina, a pichação pode caracterizar crime de dano ou, dependendo das circunstâncias do crime, concorrência desleal, prevista em lei especial.

5.10. Envio de mensagens não solicitadas

Também conhecido como *spam*, consiste no envio de mensagens não solicitadas por qualquer meio, principalmente *e-mail*, e que de algum modo possam causar dano ou prejuízo a outrem. Não existe legislação no Brasil para o *spam*[30].

5.11. Uso indevido informático

Uso indevido de sistemas informáticos, ainda que autorizado, com possibilidade de prejuízo a titular ou cessionária do sistema, prejudicando seu funcionamento, ou mesmo causando prejuízo a outras pessoas que utilizam o sistema, atentando contra seu perfeito funcionamento ou disponibilidade. Embora tenhamos fragmentos, não se tem um único tipo penal que se amolde com simetria na conduta informática.

6.

DIREITO PENAL INFORMÁTICO

Conhecidas as técnicas pelas quais se podem praticar comportamentos ou condutas informáticas, que podem ser consideradas crimes digitais, bem como apresentada uma proposta (TCC) para legislação eficaz em sede de direito penal informático, apresentamos neste capítulo um estudo pormenorizado sobre o Direito Penal Informático, a seguir detalhado, apresentando ainda uma classificação para os crimes informáticos.

6.1. A tutela aos bens informáticos

Sempre foi um desafio tratar de crimes informáticos com um Código Penal da era do Rádio. Nosso Decreto-Lei n. 2.848/40, embora tutele a maioria dos delitos informáticos, é omisso em questões onde a informática deveria ser o bem protegido pelo Direito Penal.

Não se tratava a informática como um bem jurídico relevante, merecedor da tutela do Direito Penal. O desenvolvimento da tecnologia concebeu uma sociedade denominada "da informação", altamente dependente da informática, que lhe serve para base e ambiente de relações jurídicas. Foi quando o Direito passou a reconhecer outros valores penalmente relevantes. Começaram-se as discussões sobre normas protetoras dos direitos dos cidadãos em face das novas tecnologias e do uso mal-intencionado destas.

Considerando que o direito só deve agir preservando os bens mais relevantes e imprescindíveis das relações sociais, intervindo minimamente na vida do cidadão, não foi fácil aprovar legislação que tipificasse crimes cibernéticos. Em tal contexto, em que pese a sabida proteção oferecida aos bens jurídicos tradicionais, era preciso proteção diante dos delitos cometidos em face de bens

jurídicos informáticos.

Novas figuras delitivas no Código Penal, embora no nosso sentir não resolvam o problema da falta de estrutura investigativa, sem dúvida alguma eram clamadas por autoridades e operadores do Direito. E elas surgiram.

De fato, é inegável que onde há relevância econômica deve haver relevância jurídica, e é esta a tutela que se apresenta, a proteção à incolumidade de informações, bancárias, financeiras, dentre outras informações geradas e tratadas por pessoas físicas e jurídicas. Sistemas informáticos processam ou tratam dados eletrônicos, geram significado e informações. Logo, são merecedores da tutela penal, pois informação é bem precioso.

Como salienta Ferreira Lima (2011, p. 6), diante da evolução tecnológica existe uma predisposição social em reconhecer bens jurídicos informáticos e, dentre os que mais se sobressaem, temos o sigilo e a segurança de dados e informações eletrônicas. Para a autora, é tal juízo de reprovação (violação a dados e a informações privadas) que move o Direito Penal. De fato, tal juízo de reprovação existia, mas foi preciso que uma pessoa pública, atriz popular, fosse vítima de um suposto crime informático para que o legislativo finalizasse uma discussão de mais de 10 (dez) anos no Congresso Nacional, com a aprovação da Lei n. 12.737/2012, sancionada em 30 de novembro do mesmo ano.

Elevaram-se, pois, os dados informáticos e os dispositivos ao *status* de valores jurídicos fundamentais das relações sociais de uma sociedade dependente da tecnologia da informação, protegendo-os. Assim, ao tratarmos de “crime informático”, usamos tal nomenclatura justamente para demonstrar qual o bem jurídico protegido pelo Direito Penal, a informática, ou a privacidade e a integridade dos dados informáticos.

6.2. Conceito jurídico de crime informático

Crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciam diretamente no Direito Penal.

As recomendações da *Organization for Economic Cooperation and Development* (OECD), de 1986, conceituam crime eletrônico (SCHJOLBERG, p. 8) no seguinte sentido: "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, transmissão de dados, podendo implicar a manipulação de dados ou informações, a falsificação de programas, o acesso e/ou o uso não autorizado de computadores e redes".

Fabrízio Roza (2007, p. 53), ao tratar da denominação envolvendo crimes cibernéticos, bem pontua que "Klaus Tiedemann fala em 'criminalidade de informática' para designar todas as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador. Aqui, Tiedemann engloba, por um lado, os problemas da esfera privada do indivíduo que possa ser ameaçada pela memorização, interconexão e transmissão informática de dados, e, por outro lado, os atentados ao patrimônio cometidos através de computadores ou sistemas. Kohn utiliza *computer criminals* para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a 'infrações cometidas por meio de computador'. Há ainda quem prefira a expressão 'crimes de computador', 'cybercrimes', 'computer crimes', 'computing crimes', 'delito informático', 'crimes virtuais', 'crimes eletrônicos' ou ainda 'crimes digitais', 'crimes cibernéticos', 'infocrimes', 'crimes perpetrados pela Internet', denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa".

Há, na doutrina, uma distinção entre delitos informáticos e criminalidade na Internet. Rodríguez Mourullo, Alonso e Lascuraín (apud FERREIRA, 2004, p. 52), ao tratarem de crimes informáticos, apresentam interessante distinção: os delitos informáticos teriam como objeto de ataque um elemento informático, ou seja, dados e/ou sistemas informáticos, enquanto a criminalidade na Internet seria o instrumento do delito.

Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e

antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

No Brasil, escolheu-se nomear os crimes cometidos contra a informática de "delitos informáticos", termo usual em países de língua espanhola que se relaciona à ideia de proteção do objeto jurídico informática e informação.

Tem-se, pois, que informática é a ciência dedicada ao tratamento da informação mediante o uso de computadores e demais dispositivos de processamento de dados. E, neste sentido, a boa prática impõe que os tipos sejam nominados de acordo com o bem jurídico que visam proteger.

O crime virtual, em tese, era considerado um crime-meio, em que se utiliza um meio virtual. Assim reforçava Patrícia Peck Pinheiro (2007, p. 250; 2014, p. 307): "Não é crime-fim por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros".

Entendemos diversamente. O crime virtual pode ser um crime-meio, mas vem se desenvolvendo como crime-fim, o que demandou, aliás, a tipificação de alguns crimes informáticos próprios, com a edição das Leis n. 12.735/2012 e n. 12.737/2012. Ademais, não só *hackers* podem praticar um crime-fim informático, mas qualquer pessoa.

Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não[31].

A exemplo, tem-se como crimes mais comuns praticados na rede o estelionato e a pornografia infantil e os ataques mais comuns os praticados por meio de vírus de computador ou *malware*, seguido de invasão de perfis nas redes sociais e por ataques de *phishing*. Já os crimes cibernéticos mais raros (porém crescentes) continuam sendo aqueles causados por códigos maliciosos, negação de serviço, dispositivos roubados, sequestrados e roubo de informações privilegiadas. Quando

combinados, esses fatores são responsáveis por mais de 78% dos custos anuais com crimes cibernéticos para as organizações[32].

Como visto, em que pese o Direito Penal já proteger certos bens jurídicos agredidos via informática, fato é que os dados e a segurança dos sistemas e redes informáticos clamavam por uma proteção específica.

6.3. Classificação dos crimes informáticos

Pode-se classificar o Direito da Informática em Direito Civil da Informática e Direito Penal da Informática. Direito Civil da Informática é o que atrai as normas, regulamentações e entendimentos jurídicos atinentes às relações privadas oriundas ou realizadas por intermédio da tecnologia da informação. Já o Direito Penal da Informática é o complexo de normas, regulamentos e entendimentos jurídicos concebidos no escopo de repreender fatos criminosos que atentem contra bens informáticos.

No mundo, muitos doutrinadores procuraram classificar os crimes digitais. No que tange à nomenclatura, "Kohn utiliza *computer criminals* para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a 'infrações cometidas por meio de computador'. Há ainda quem prefira a expressão 'crimes de computador', 'cybercrimes', 'computer crimes', 'delito informático', 'crimes virtuais', 'crimes eletrônicos' ou, ainda, 'crimes digitais', 'crimes cibernéticos', 'infocrimes', 'crimes perpetrados pela internet', denominações distintas, mas, que, no fundo, acabam por significar basicamente a mesma coisa" (ROZA (2007, p. 53).

Dentre as classificações mais conhecidas e clássicas, temos as seguintes:

Klaus Tiedemann (1980, p. 122-129, *apud* CRESPO, 2011, p. 60), autor que tratou na década de 1980 da criminalidade informática no âmbito dos delitos econômicos, classificou os crimes digitais, em sua visão "criminalidade informática", em:

a) *manipulações*: podem afetar o *input* (entrada), o *output* (saída) ou mesmo o processamento de dados;

b) *espionagem*: subtração de informações arquivadas, abarcando-se, ainda, o furto ou emprego indevido de *software*;

c) *sabotagem*: destruição total ou parcial de programas;

d) *furto de tempo*: utilização indevida de instalações de computadores por empregados desleais ou estranhos.

Ulrich Sieber (2008, *apud* CRESPO, 2011, p. 60) emitiu parecer para a Comissão Europeia sobre crimes informáticos, classificando-os em:

a) violação à privacidade;

b) crimes econômicos:

b.1) *hacking*;

b.2) espionagem;

b.3) pirataria em geral (cópias não autorizadas);

b.4) sabotagem e extorsão;

b.5) fraude;

c) conteúdos ilegais e nocivos;

d) outros ilícitos;

d.1) contra a vida;

d.2) crime organizado;

d.3) guerra eletrônica.

Martine Briat (1985, p. 287), autora francesa, buscou classificar os delitos informáticos em crimes onde a informática é o meio para a prática delituosa, e os demais delitos, onde, nesta categoria, citamos:

a) manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;

b) falsificação de dados de programas;

c) deterioração de dados e de programas e entrave à sua utilização;

d) divulgação, utilização ou reprodução ilícita de dados e de programas;

e) uso não autorizado de sistemas de informática; e

f) acesso não autorizado a sistemas de informática.

Davara (apud FERREIRA, 2004 , p. 53) apresenta interessante classificação para as diferentes ações delitivas virtuais, a seguir detalhada:

a) manipulação de dados ou informações contidos nos arquivos ou suportes informáticos alheios;

b) acesso aos dados e/ou sua utilização por quem não está autorizado;

c) introdução de programas ou rotinas em outros computadores para destruir informação, dados ou programas;

d) utilização de computadores e/ou programas de outra pessoa com o fim de obter benefícios em prejuízo de outros;

e) utilização de computadores com fins fraudulentos;

f) agressão à privacidade mediante a utilização e processamento informático de dados pessoais com fim distinto ao autorizado.

Rovira del Canto (2002, p.128), por sua vez, tem uma das classificações mais amplas sobre delitos informáticos, sendo elas:

a) infrações à intimidade;

b) ilícitos econômicos;

c) ilícitos de comunicação ou difusão de conteúdos ilegais ou perigosos;

d) outros delitos.

Em nosso sentir, a classificação mais precisa se assemelha à proposta por Briat (1985), diga-se, a distinção entre crimes informáticos em que a informática é o meio para a prática de velhos crimes ou

agressão a bem jurídico protegido pelo Direito Penal, e crimes informáticos em que a informática (inviolabilidade dos dados) é o bem jurídico protegido, propriamente dito.

Estas classificações podem se fundir, como, por exemplo, no delito em que um bem jurídico informático é agredido para que o agente possa cometer o crime-fim, diga-se, agredir outro bem jurídico, ou mesmo no caso em que da agressão ao bem jurídico informático outros bens também são afetados, ainda que não informáticos. Imaginemos, por exemplo, a hipótese onde o agente invade dispositivo alheio e altera informação fazendo a pessoa ser classificada como procurada pela polícia. Danos maiores podem advir.

Assim, classificamos os crimes informáticos em:

a) *crimes informáticos próprios*: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;

b) *crimes informáticos impróprios*: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;

c) *crimes informáticos mistos*: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;

d) *crime informático mediato ou indireto*: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto).

De outra ordem, releva assinalar as importantes lições de Crespo (2011, p. 63) acerca da

conceituação de crime informático: “A simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser – repita-se – com precisão técnica, considerada um crime informático. Ocorre, todavia, que não só autores, mas também as mídias em geral, convencionaram denominar crimes informáticos qualquer delito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito. Destarte, apesar de não ser a mais técnica, a nosso ver, é impossível ignorá-la, dada sua particular popularidade acadêmica e, por que não, social, vez que mesmo a mídia em geral passou a se valer dessa mesma classificação”.

Resta assinalar, pois, que os novos tipos penais previstos na Lei n. 12.737/2012 são crimes afetos, via de regra, à categoria de crimes informáticos próprios, onde o bem jurídico protegido é a segurança dos dispositivos e dados informáticos.

6.4. Crime informático no âmbito internacional

De forma a conjugar esforços no combate aos crimes eletrônicos, foi realizada a chamada Convenção de Budapeste, acerca de cibercrimes, no âmbito do Conselho da Europa. Trata-se, pois, de documentação de Direito Internacional Público, elaborada por comitê de especialistas, no escopo de que os países signatários implementem normas de direito material que façam frente ao crime cibernético.

Assim, tem-se como um acordo internacional, firmado em 23 de novembro de 2001 por países da União Europeia, já contando com a adesão de Austrália, Japão e Estados Unidos, que fixa diretrizes às políticas nacionais e propõe a harmonização das legislações para que se possa combater o cibercrime de maneira eficiente[33].

O Brasil não aderiu à Convenção de Budapeste. Igualmente, não se pode prever que com as Leis n. 12.735/2012 e n. 12.737/2012 possa o país realizar a precitada adesão, eis que outros crimes digitais continuam desprovidos de um tipo penal próprio. Tem-se, porém, com tais leis, um avanço local e um passo para que o país possa estar em futura conformidade com a precitada Convenção[34].

Traz o tratado (Convenção de Budapeste) cinco títulos relacionados a direito material, cinco títulos envolvendo direito processual e mais tópicos envolvendo cooperação internacional, resolução de conflitos, consulta entre as partes etc.

Em que pese o Brasil não aderir ao precitado documento, é fato que o mesmo documento impulsionou os debates e o trâmite do Projeto da Lei n. 2.793/2011, transformada na Lei n. 12.737/2012, sobretudo o Título 1 da Convenção, que trata das infrações relacionadas com a confidencialidade, integridade e disponibilidade dos sistemas informáticos e dados informáticos.

Assim, dentre as diretrizes aos países que pretendem legislar sobre crimes eletrônicos, temos, na Convenção de Budapeste, pontos em que verificamos claramente a influência de tal texto na Lei n. 12.737/2012.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such

computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i – a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii – a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may

require by law that a number of such items be possessed before criminal liability attaches.

2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article[35].

Deste modo, verifica-se que a recém-aprovada Lei brasileira n. 12.737/2012 é fortemente influenciada pelos preceitos da Convenção de Budapeste.

6.5. Perfil do criminoso digital

Não se pode traçar um perfil cartesiano sobre o criminoso cibernético. Sabe-se, porém, que o crime cibernético no Brasil está menos técnico e muito mais criativo.

Décadas atrás, um criminoso digital estava relacionado diretamente ao conceito de *cracker*, pessoa com conhecimentos profundos das intimidades de um computador ou dispositivos computacionais, conhecedora de redes, protocolos, programação de baixo nível, dentre outras habilidades.

Este cenário foi modificado. A realidade, hoje, é que grande parte dos crimes digitais se deve à ignorância dos usuários, despreparo das autoridades investigativas e, principalmente, à banalização e difusão das técnicas e ferramentas para aplicação de golpes. Pode-se dizer também que os criminosos digitais, em sua maioria, não praticariam crimes do mundo real, porém interessam-se pela prática delituosa virtual, amparados pela falsa sensação de anonimato e conhecedores do despreparo das autoridades em investigarem delitos desta natureza.

Neste cenário, podemos elencar o crescente número de adolescentes, até mesmo de classes média

e alta, cada vez mais envolvidos com crimes cibernéticos.

Este criminoso digital também pode ser considerado "atacante" ou autor da fraude. Esta fraude, quando praticada contra empresas, pode ser: a) interna, praticada por empregado, preposto ou pessoa dentro do local fraudado (*insider*); ou b) externa, onde o fraudador, que pode ser um criminoso digital, não tem vínculo, no momento da fraude, com o local fraudado (*outsider*).

Logo, muito se fala em "crimes de alta tecnologia" quando, na verdade, a tecnologia utilizada na maior parte dos casos é trivial[36], corriqueira, de fácil curva de aprendizagem, e com ferramentas disponíveis para venda e troca em redes IRC (*Internet Relay Chat*) e demais cantos da Internet. Horas de vídeos disponíveis na Internet podem conduzir pessoas a praticarem invasões com relativa facilidade. As vítimas comumente contribuem e cooperam ativamente para se tornarem vítimas, facilitando o trabalho do cibercrime.

Como verificado, não existe consenso para um perfil para o criminoso digital (embora existam importantes estudos e pesquisas a respeito[37]) e, na sua maioria, os crimes não são de "alta tecnologia". Muito se comenta ou classifica-se o crime digital no conceito de colarinho branco, diga-se, crimes que somente pessoas com determinado *know-how* podem praticar, porém, é fato que tais premissas se minimizam a cada dia, onde cada vez mais pessoas sem sólidos conhecimentos em informática iniciam a prática delitiva, obtendo êxito.

6.6. Sujeito ativo do crime informático

Como se viu, não existe consenso em relação ao perfil do criminoso digital. Para alguns, seriam jovens; para outros, a oportunidade fez com que qualquer pessoa pudesse ser um criminoso digital em potencial; para outros, ainda, a motivação na década de 1980, que era a "emulação", cede espaço a motivação do século XXI, o dinheiro.

No ano 2000, Mauro Marcelo Lima e Silva (2004, p. 3) realizou este exercício ao afirmar que "geralmente, os criminosos são de oportunidade e os delitos praticados por agentes que, na maioria

das vezes, têm a sua ocupação profissional ligada à área de informática. O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, 'uma brincadeira'. Mais: preferem ficção científica, música, xadrez, jogos de guerra e não gostam de esportes, sendo que suas condutas geralmente passam por três estágios: o desafio, o dinheiro extra e, por fim, os altos gastos e o comércio ilegal".

Muitos utilizam o termo *hacker* para se referirem ao criminoso digital. Explica-se. Nos dizeres de Lima (2011, p. 42), "a expressão *hacking*, para Charles C. Palmer, diretor do Global Security Analysis Lab., é 'o uso não autorizado do computador e de seus recursos de rede (o termo *hacker* originariamente significava um habilidoso programador. Recentemente, com o fácil acesso a múltiplos sistemas, tem uma conotação negativa)'". Prossegue o autor, criticando que "essa conduta havida por alguns como inofensiva, vez que há *hackers* que acessam sistemas apenas pelo desafio, pode ser comparada à entrada de um estranho na sua casa, que a tudo olha, toca e depois sai".

Não podemos consentir com esta cultura. Um *hacker* é um profundo conhecedor de informática, podendo ser um profissional de segurança da informação ou pesquisador, que não utiliza seus conhecimentos para fins ilegítimos. Assim, é erro grave classificar *hacker* como um bandido. Na verdade, qualquer pessoa pode cometer um crime digital. Uma pessoa pode cometer um crime virtual sem conhecer sequer uma linha de programação. A Engenharia Social (práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas) vem se demonstrando importante arma para a prática de crimes virtuais.

Marcelo Crespo (2011, p. 95) estabelece uma classificação, advertindo que nem sempre os *hackers* são os vilões da Internet, mas que, em verdade, existe uma série de denominações para

identificar os responsáveis por condutas ilícitas. Dentre as nomenclaturas existentes, podemos citar:

a) *Hackers*: Fuçador. Expressão que surgiu nos laboratórios do MIT (*Massachusetts Institute of Technology*). Qualquer um que tenha grande conhecimento sobre tecnologia e que faça invasões.

b) *Carders*: Estelionatários especializados em fraudes com cartões.

c) *Crackers*: Seriam os verdadeiros criminosos da rede. Utilizam seus conhecimentos de tecnologia para más finalidades.

d) *Phreakers*: São os "*hackers* da telefonia", capazes de realizar interceptações, paralisar serviços e até mesmo utilizar a telefonia em nome de terceiros.

Outra classificação existente seria entre *White Hats, Gray Hats* e *Black Hats*. *Black Hats* são os *crackers*, pessoas com elevados conhecimentos de tecnologia que os utilizam para atividades criminosas. *White Hats* seriam os *hackers*, ou ainda "*Hackers*" *éticos*, especialistas que usam suas habilidades para o bem e para o fortalecimento da segurança dos sistemas. Teremos ainda os *Gray Hats*, que se encaixaria em algum lugar entre o *Black* e o *White Hat*. O melhor conceito que identificamos sobre *Gray Hat* está nos exemplos de Russo (2013, p. 4), que esclarece:

"Um *hacker* de chapéu branco primeiramente pede permissões à corporação ou empresa antes de testar a segurança de *sites*, *softwares* ou sistemas. Caso descubra alguma falha em sua exploração, o mesmo alerta sigilosamente todos os envolvidos após comprometê-los. Já o *Hacker* de chapéu cinza não utiliza o seu acesso indevido para fins maléficos, mas caso ele acesse um sistema de segurança, o mesmo já está comprometido, fato que torna a ação do *Hacker Gray Hat* totalmente ilegal.

Se um *hacker* de chapéu cinza descobre uma falha de segurança em um *software* ou *site*, o *Hacker Grey Hat* pode revelar esta falha publicamente para a empresa do sistema invadido, ao invés de divulgar em particular aos responsáveis como o *White Hat* faria. Deste modo eles não iriam se aproveitar da falha de segurança para seu próprio benefício".

Também classificam-se os que não possuem conhecimento em informática, mas pensam que têm. São eles os *Lammers* e os *Wannables*. Sob o prisma de uma defesa criminal, demonstrar que o

cliente é um *Lammer* tem o seu sentido, pois poderia ser importante prova a atestar a ausência de autoria de um crime informático, como a invasão, por exemplo.

6.7. Competência e lugar do crime informático

A questão da territorialidade encontra guarida nos Códigos Penal e de Processo Penal brasileiros, embora seja tema considerado de relativa controvérsia.

Determinar a territorialidade implica determinar o juiz competente para processar e julgar um delito informático. Pontua-se que o Direito Penal brasileiro está relacionado ao território nacional, e o que se procede fora de tais limites resulta em revisão dos acordos entre os países. No Brasil, a legislação que norteia a questão está relacionada nos arts. 5º, 6º e 7º do Código Penal.

Destaca-se que, caso o crime informático seja praticado contra bens da União, a competência será da Justiça Federal; igualmente, nos casos em que por Convenção ou Tratado o Brasil se obrigou a reprimir (art. 109, IV e V, da Constituição Federal).

No que tange ao lugar do crime, o Código Penal adotou, em seu art. 6º, a teoria da ubiquidade, sendo considerado o lugar do crime o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria se produzir o resultado. Deste modo, ao se considerar alguém, no Estado do Rio de Janeiro, que invade o computador de outrem, localizado em São Paulo, teríamos o juízo onde está o dispositivo invadido como competente para processar e julgar o delito informático.

Já no que diz respeito a condutas ilícitas praticadas em território estrangeiro, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deverá ser tratada pela extradição.

Logicamente que a autoridade brasileira é competente para processar um crime digital praticado por agente brasileiro no exterior, com vítima no Brasil, mas dependerá que este agente adentre território nacional. Logo, crimes cometidos por meio de *proxies, vpns*, entre outros recursos para

mascarar a origem da conexão, onde o agente está no Brasil e só se vale de uma conexão do exterior, podem ser processados aqui, desde que, claro, identificado o criminoso. E aí reside mais um problema, pois provedores estrangeiros muitas vezes se recusam a fornecer dados de acesso a aplicações feitas por brasileiros, mas armazenados no exterior.

De modo esclarecedor, assim pontua Ferreira (2004, p. 77), a respeito do tema: “Damásio Evangelista de Jesus (apud VALIN, 2000, p. 117) entende que, para casos relacionados à Internet, deveria ser adotado algo semelhante à teoria da atividade que, como visto, determina como sendo o local do crime aquele em que o agente praticou o delito. Pensamento contrário é defendido por Valin (2000, p. 117), que acredita ser a melhor solução considerar-se como local do crime aquele em que está o autor das infrações, pois o referido país teria melhores condições de aplicar eventual pena, sem necessidade de discussão sobre extradição, no máximo se discutiria o cumprimento dos efeitos cíveis da condenação no sentido de retirar da rede o material publicado, o que talvez possa gerar a necessidade de um novo processo em país distinto ao da condenação”.

Importa dizer ainda que, nos termos do § 2º do art. 70 do Código de Processo Penal, quando atos executórios tenham ocorrido fora do Brasil, a competência será do local onde a infração se deu ou foi concluída a ação delituosa (resultado).

É importante ponderar, no entanto, que, em se tratando de crimes praticados por brasileiros no exterior que façam vítimas no Brasil, por questões de soberania, a conduta praticada pelo agente deve ser considerada ilícita em ambos os países, bem como deverá o agente ingressar em território nacional para que seja processado (art. 7º, II, § 2º, *a* e *b*, do Código Penal).

6.8. Reflexão sobre a necessidade de uma legislação específica

Uma corrente que defendia o “direito penal mínimo” justificava a não necessidade de legislação, afirmando que 95% dos crimes eletrônicos já eram previstos no Código Penal brasileiro.

Neste sentido, Alexandre Jean Daoun (2011, p. 2) justifica que “a tônica principal é a seguinte: a

desnecessidade de legislação penal nova, o direito penal para as relações virtuais é um direito penal mínimo. É isso que se recomenda. Minimamente usar o direito penal, sendo que se devem usar outros ramos do Direito para coibir as situações praticadas no ambiente eletrônico. Direito Penal deve ser guardado e resguardado para situações absolutamente extremas. Daí a crítica a essa compulsividade de legislar, de criar lei penal para isso, para aquilo, porque o Direito Penal é o instrumento mais drástico que se tem. Pagar uma indenização é uma coisa, perder a liberdade é outra. Então, para não se perder a credibilidade, é direito penal mínimo. E no ambiente virtual, 95% das relações que se tem já são disciplinadas na legislação penal. Não há por que criar e falar tanto em legislação penal específica".

Como sabemos, a informática trouxe em seu bojo novas formas de realizar velhos crimes. Ameaça será sempre ameaça, difamação sempre será difamação, estelionato sempre será estelionato, não importando se praticados por intermédio do computador ou não.

Sob outro aspecto, também é inegável que crimes informáticos puros hoje atentam contra bens jurídicos não protegidos pelo Direito Penal. A necessidade de enquadramento penal sempre foi debatida entre operadores do Direito Penal, especificamente se devemos conceber leis específicas ou adaptarmos a legislação vigente.

Ao que parece, no Brasil, o legislador criminal pátrio caminha no sentido das alterações do Código Penal e do Código de Processo Penal, ao invés de leis específicas. Tal premissa se justifica com o Projeto de Lei n. 933/99, de autoria do Poder Executivo, que criou a Lei n. 9.983, de 14 de julho de 2000, nascida a princípio para proteger os sistemas da previdência social, e que posteriormente abrangeu toda a Administração Pública, alterando o Código Penal para fazer prever as seguintes disposições envolvendo informática:

a) no crime de divulgação de segredo, previsto no art. 153 do Código Penal, acrescentou o § 1º-A, punindo com detenção de um a quatro anos mais multa aquele que divulga, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de

informações ou bancos de dados da Administração Pública;

b) criação de dois novos tipos penais, a “inserção de dados falsos em sistemas de informações”, art. 313-A, com pena de reclusão de dois a doze anos mais multa, e a “modificação não autorizada de sistema de informações”, prevista no art. 313-B, cominando pena de detenção de três meses a dois anos mais multa;

c) a alteração do art. 325 do Código Penal, crime de violação de sigilo funcional, para acrescentar os §§ 1º e 2º, passando a punir com reclusão de dois a seis anos e multa quem permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública ou quem se utiliza indevidamente do acesso restrito.

Neste cenário, embora seja uma lei muito criticada, que mais se destacou pelo “alerta” sobre os crimes eletrônicos do que contribuiu para o chamado “controle de criminalidade”, é inegável que marcou a tendência do legislador em alterar o Código Penal já existente. Tal assertiva é reforçada, doze anos depois, com a promulgação das leis objeto deste livro, n. 12.735/2012 e n. 12.737/2012 (Lei Carolina Dieckmann).

6.9. Legislação penal informática no mundo

Apresenta-se, na sequência, uma síntese de alguns países do mundo que vêm regulamentando a questão dos crimes informáticos.

6.9.1. Estados Unidos

Um dos países que primeiro legislaram sobre crimes informáticos no mundo. Os debates se iniciaram na década de 1970, e na década de 1980 era promulgada a *Computer Fraud and Abuse Act*, publicada em 1986.

Conforme explica Crespo (2011, p. 155), embora tenha sido a Suécia o primeiro país a criar norma

incriminadora para ofensas a bens “informáticos”, foram os Estados Unidos os precursores do verdadeiro combate à criminalidade informática, o que se deu nos patamares estadual e federal.

A legislação foi alterada e hoje temos outras leis que tratam da questão informática. No *United States Code,* Título 18, Parte I, Capítulo 47, que trata da fraude e declarações falsas, Seção 1030, temos os crimes envolvendo fraude e atividades relativas em conexão com computadores.

Outros capítulos do USC tratam também de crimes informáticos[38]. A lei pune casos de acesso indevido, interceptação não autorizada e sabotagem informática. Conceitua ainda, a Lei Federal americana, a fraude de computador, como o uso do computador para criar uma deturpação desonesta de um fato como uma forma de induzir alguém a fazer ou deixar de fazer algo que lhe cause uma perda.

Verificamos na legislação americana que é condição, nos crimes de acesso indevido, que o agente tenha obtido os dados ou causado dano, punindo esta quem *intencionalmente acessa um computador protegido ou sem autorização e, como resultado de tal conduta imprudente, causa danos.*

Importante mencionar que, em 1994, o Código Penal Federal fora alterado pelo *Violent Crimes Act* – Lei de Crimes Violentos, que tipificou condutas como dano a dados e sistemas, disseminação de vírus e interceptação telemática. Mais tarde, em 2001, a Lei Federal também é emendada pela Lei Patriótica – *USA Patriot Act*, que, no escopo de combater o Terrorismo, mune o governo de possibilidade e estruturas legais para o monitoramento e interceptação telemática.

Destaca-se, igualmente, que nos Estados Unidos os Estados podem criar suas legislações em matéria criminal. A lei federal tem papel secundário. Caso célebre de aplicação da lei de crimes informáticos americana envolveu o ativista e programador Aaron Swartz, que foi preso por autoridades federais em 6 de janeiro de 2011, após utilizar a rede do MIT para descarregar, sem pagar por isso, grandes volumes de artigos científicos de uma revista. Foi acusado pelo crime de invasão de computadores, por “ter usado formas não convencionais de acesso ao repositório da revista”. Suas condutas violariam 11 dispositivos da Lei de Crimes Informáticos norte-americana e

talvez sofreria uma penalidade de mais de 1 milhão de dólares. Matou-se em 11 de janeiro de 2013. O acesso a sistemas informáticos por meio de formas não convencionais necessariamente é invasão? Em nosso sentir, não. Se em vez de utilizar um formulário de pesquisa disposto, realizamos diretamente uma pesquisa no banco de dados, desprotegido, não há que se falar em invasão alguma.

6.9.2. Filipinas

Em janeiro de 2012, o Senado aprovou a redação final da *Bill 2976*: *The Cybercrime Prevention Act of 2012*[39], que insere tipos na legislação criminal tratando de temas como *cybersex* e *cybersquatting*.

6.9.3. Emirados Árabes

Legislação foi promulgada em 2012, punindo condutas como o uso da Internet para transmitir, publicar e promover atos pornográficos e atos indecentes.

6.9.4. Itália

Na Itália, as discussões sobre crimes informáticos se deram entre 1992 e 1993, com a edição do Decreto Legislativo n. 518, de 29 de dezembro de 1992, e Lei n. 547, de 23 de dezembro de 1993, onde tipos penais tiveram redação ampliada para contemplar crimes informáticos. Passou a criminalizar condutas como a sabotagem informática, que corresponde ao ataque à funcionalidade de sistema informático, e fraude informática, que consiste em alterar dados em sistemas alheios para obter vantagem. Interessante ponto vem previsto no art. 615 do Código Penal, dos crimes contra a inviolabilidade de domicílio, onde o tipo foi ampliado para abranger também os casos envolvendo o crime de “invasão de IP” que vise dano a sistema alheio. Invasão de computadores é considerada violação de domicílio.

6.9.5. Alemanha

É considerada o primeiro país a refletir alterações legislativas em relação a crimes informáticos. Desde 1986, a Lei de Criminalidade Econômica contempla condutas informáticas como espionagem, fraude informática, falsificação de dados, alteração de dados e a sabotagem informática. Em setembro de 2006 o Governo propôs um novo projeto para atualizar a legislação informática, ainda em andamento. No atual *Strafgesetzbuch* (Código Penal Alemão[40]), temos a Seção 202a, que cuida de espionagem, a Seção 303a, que trata do crime envolvendo alteração de dados, e a Seção 303b, que trata da sabotagem informática. Em 19 de agosto de 2014 o país apresentou um projeto de Lei de Segurança Cibernética, para proteção de infraestrutura crítica do país e proteção dos cidadãos em geral.

6.9.6. China

A lei denominada *Computer Information Network and Internet Security, Protection and Management Regulations* foi publicada em dezembro de 2011. Em alguns tipos penais, pode haver até mesmo o cancelamento da conta do usuário junto ao Provedor de Acesso à Internet. Os tipos previstos na legislação criminal chinesa incluem a sabotagem, o acesso indevido, a alteração de dados e o uso de computadores para fraudes, corrupção, criação e propagação de vírus, desvio de fundos públicos, roubo, roubo de segredos do Estado, dentre outros.

6.9.7. Índia

Na Índia, temos a *The Information Technology Act (21/2000),* que pune o *hackerismo* com pena superior a três anos, bem como a sabotagem ou alteração indevida de sistemas informáticos.

6.9.8. Japão

O Japão possui regulamentações envolvendo crimes cibernéticos na Lei n. 128/99, denominada *Unauthorized Computer Access Law* e nos arts. 258 e 259 do Código Penal. Dentre os crimes previstos está a invasão de dispositivos informáticos, revelação de senha ou de código de acesso. As penas incluem trabalhos forçados e valores acima de 500 mil yens.

6.9.9. França

Desde 1988, com a Lei n. 19, tínhamos disposições sobre crimes informáticos, com elementos que tipificavam o acesso fraudulento a um sistema de dados, sabotagem informática, com a falsificação ou adulteração de um sistema de tratamento de dados, destruição de dados e a falsificação de documentos informatizados.

Modernamente, temos a *Loi 575, du 21 juin 2004*[41], que visa garantir o comércio eletrônico e que trata também de punições a fraudes informáticas. A França, igualmente, ratificou a Convenção Europeia do Cibercrime em 10 de janeiro de 2006. No país ainda existe a chamada Lei HADOPI (do francês *Haute Autorité pour la Diffusion des œuvres et des droits la Proteção d'auteur sur Internet),* de 2009, apoiada pelo então presidente Nicolas Sarkozy, que para proteção de direitos autorais previa a suspensão do acesso à Internet de um violador reincidente, disposição esta que foi revogada em 8 de julho de 2013. Desde a aprovação da lei até a revogação do dispositivo, tem-se relatos de apenas um usuário que foi suspenso da Internet (por 15 dias) e multado (em 600 euros). No entanto, a lei obriga os provedores a fornecer dados dos usuários se requisitados judicialmente.

A legislação criminal francesa pune: a) acesso ou permanência indevida total ou parcial em sistema de processamento de dados – com pena de dois anos de prisão mais multa de 30.000 euros, b) supressão ou modificação de dados em sistemas informáticos, bem como a introdução fraudulenta de dados – com pena de cinco anos de prisão e multa de 75.000 euros; c) comercialização, importação, posse, oferta, venda ou disponibilização de equipamento, ferramenta, programa de computador ou dados adaptados para o cometimento dos crimes informáticos – punível com as penas

previstas dos crimes-fins; d) formação de grupo ou conspiração para a prática dos crimes informáticos – punível com as penas previstas nos crimes ou na pena mais alta.

A lei francesa criminaliza o desenvolvimento e fornecimento em geral de ferramentas, equipamentos, *softwares* e códigos para a prática de crimes digitais.

6.9.10. Inglaterra

Desde 1984 o país já contava com a *Data Protection Act*, legislação que protegia os dados pessoais em ambiente informático.

A lei inglesa data de 1990. Introduziu no ordenamento jurídico o delito de acesso não autorizado com a intenção de modificar conteúdo de sistema, impedindo a operação de qualquer computador, impedindo ou dificultando o acesso a qualquer programa, impedindo a confiança nos dados, impedindo a execução de qualquer dos programas.

Trata-se de uma lei que pune, tal como a lei brasileira (12.737/2012), a conduta de invadir com a finalidade de modificar o conteúdo de computador, independentemente do resultado. Logicamente, a lei inglesa foi duramente criticada.

De outra ordem, o interessante na lei inglesa é que esta traça parâmetros ou traz comportamentos que, se praticados, indicam que a conduta efetivamente era dolosa, ou seja, indicam a provável existência de intenção de modificar conteúdo de computador. Esses parâmetros, fundamentais, não existem na lei brasileira e ficarão a cargo do magistrado.

A *Computer Misuse Act*, de 29 de agosto de 1990[42], a principal iniciativa legislativa em termos de direito penal informático, foi alterada em 2006 pelo *The Police and Justice Act 2006*. A legislação inglesa do País de Gales trata de diversos crimes, dentre os quais o acesso indevido e a produção de sistemas e código que permitam a invasão. Recentemente, em 2014, foi proposto no Parlamento 11 novas leis, dentre as quais a *Serious Crime Bill*, que poderá alterar a lei de 1990 com propostas de pena de prisão perpétua para crimes cibernéticos.

6.9.11. Portugal

Em Portugal, temos a Lei n. 109, de agosto de 1991, de crimes informáticos, que pune o acesso indevido a sistemas informáticos, classificando como uma qualificadora a conduta que é realizada com a quebra de segurança.

Dentre os crimes previstos, temos a falsidade informática, dano informático, interceptação informática, sabotagem informática (com a função de prejudicar o funcionamento informático ou comunicação de dados), acesso indevido, reprodução indevida de programas de computador etc.

6.9.12. Espanha

O Código Penal de 1995 foi alterado, prevendo diversas disposições relativas a cibercrimes, nos arts. 197, 248, 255, 256, 264, 270 e 273. Dentre alguns crimes destacamos violação de privacidade para descoberta de segredos, com pena de prisão de um a quatro anos e multa entre doze e vinte e quatro meses[43], alteração indevida de dados, acesso indevido a dados ou utilização dos dados de forma nociva ao proprietário, fraude informática (estelionato no Brasil), entre outros.

6.9.13. América do Sul

Na América do Sul, o Peru conta com o Decreto Legislativo n. 635, que pune o acesso e o uso indevido de bancos de dados, sistemas computacionais ou redes. O Código Penal peruano, ainda, pune delitos como violação de intimidade (arts. 154 e 157), delito de furto agravado pela transferência eletrônica de fundos, telemática em geral, emprego de senhas secretas (art. 186) e delito de fraude na administração de pessoas jurídicas na modalidade de uso de bens informáticos (art. 198).

No Chile, temos a Lei n. 19.223, de 7 de junho de 1993 (Lei própria de Crimes Informáticos), que pune a destruição de dados, a indisponibilização de sistemas de processamento de dados, o acesso

indevido ou uso de informações confidenciais, interceptação de dados e destruição de dados. Destaca-se que o Chile foi o primeiro país da América do Sul a atualizar sua legislação para os modernos crimes cibernéticos.

Já a Argentina possui a sua Lei de Proteção de Dados (Lei n. 25.326)[44], que inclui disposições específicas para acesso não autorizado a dados e uso indevido de dados cedidos por titulares. No que diz respeito ao Código Penal argentino, o mesmo fora alterado pela Lei n. 26.388/2008, passando a considerar e a tratar sobre crimes digitais.

6.9.14. Brasil

Como podemos verificar do direito comparado, o Brasil está bem atrasado em termos de legislação penal informática. De fato, não pairam dúvidas de que a revolução tecnológica trouxe grandes desafios ao Direito Penal, com a ocorrência de inúmeras situações em que forçosa era a subsunção dos casos trazidos à lei. Não são poucos os Projetos de Lei propostos no Congresso que tentaram tipificar condutas cometidas no mundo cibernético. Muitos, aberrações propostas por quem efetivamente longe está de entender a problemática.

E em se tratado de crimes informáticos, deve-se registrar que as características da Internet não permitiram tão somente o desenvolvimento da comunicação, mas serviram de ambiente para o crescimento de crimes de informática, estes amparados pela sensação de anonimato e pouca possibilidade de punição, considerando que, até recentemente, tudo que o Brasil tinha em termos legislativos no que diz respeito a crimes informáticos era a Lei n. 9.983/2000, que poucos artigos acrescentou ao Código Penal, aplicáveis, via de regra, a funcionários públicos. No mundo, o crime virtual já é o terceiro em prejuízo, apenas atrás das drogas e da falsificação.

Como elenca Érica Lourenço de Lima Ferreira (2005, p. 19), "na seara do Direito Penal, observa-se uma nova figura conhecida como macrocriminalidade, que rompe os limites territoriais criando uma rede de criminalidade mundial, sem respeito à soberania ou qualquer acordo internacional

realizado entre os Estados. É o caso dos crimes cometidos por meio da internet, considerado o avanço da macrocriminalidade e a dependência do sistema informático entre Estados, em virtude da globalização das informações e comunicações".

Esta globalização também é jurídica. Ao mesmo tempo que se buscam liberdades na rede, surge a consciência da necessidade de se fazer frente a ações de delinquentes cibernéticos, sobretudo no Brasil, onde se passa mais tempo na Internet do que vendo TV[45].

E fazer frente não envolve apenas tipificação ou a mera criação de leis, mas educação digital, definição do que seria "território e competência cibernética" (que passa pela problemática da jurisdição), estrutura investigativa e cooperação internacional dos intermediários e atores da Internet no Brasil, desafios que são tratados na presente obra.

Sob outra ótica, desenvolver arcabouço próprio no que tange à proteção do cidadão e seus dados em face da criminalidade informática passa a ser questão de soberania, considerando a estrutura da rede, onde muitos serviços usados por brasileiros são de empresas sediadas em solo estrangeiro. A Internet seria realmente mundial? Ou estaríamos nas mãos e sob controle de determinadas nações? Ao não dotarmos nosso povo com tecnologia, estaríamos contribuindo para uma desigualdade, para a ditadura da informação?

Não bastasse, cada vez mais somos submetidos às leis estrangeiras, eis que grandes provedores de serviços, de modo a frustrar a investigação de um delito cibernético, a evocam, como se fossem normativa pátria, impedindo o acesso de autoridades a dados de pessoas que praticam crimes no Brasil, mas que estão usando serviços de empresas do "Vale do Silício" ou sediadas em outras localidades do globo.

Augusto Bequai (apud HERRERO, 1992) já preconizava ideias de que a *tecnoética* é inexistente no mundo cibernético e que criminosos digitais exploram lacunas jurídicas de modo a escapar das investigações digitais. Que lei, por mais rígida que seja, resistiria a um bom *proxy* (sistema que permite ocultar ou alterar o real endereço IP de um usuário de Internet)?

Se lacunas jurídicas podem ser identificadas em recentes leis que tratam de crimes informáticos, o que dizer de um país que tratava o tema apenas com o Código Penal brasileiro?

No Brasil, tem-se o Código Penal de 1940 (Decreto-Lei n. 2.848), que, embora antigo, já fazia frente a grande parte dos crimes informáticos (ou, segundo alguns autores, crimes comuns cometidos por intermédio da informática). Questionou-se muito da necessidade de uma lei específica para tanto. Para muitos autores, o foco do Direito Penal é a proteção de bens jurídicos individuais, não sendo coerente a aplicação penal de interesses supraindividuais. Em tese, a conduta delitiva deveria lesionar bens pessoais e não direitos. Na era digital, porém, acentua-se a tutela penal dos direitos difusos. Passamos a considerar o objetivo da Lei Penal com o escopo de proteger a segurança e possibilitar a vida da sociedade digital. A globalização vai criando ou "inventando" novos riscos, e o Direito Penal segue avançando, desconsiderando princípios consagrados, como a intervenção mínima. Pune-se o risco aos bens jurídicos ameaçados pela informática ou pelo uso inadvertido e criminoso desta.

Dentre vários projetos de lei sobre o tema que tramitam ou tramitaram no Congresso Nacional, destacamos o Projeto de Lei n. 84/99, de autoria do então Deputado Luiz Piauhylino, apresentado em 24 de fevereiro de 1999. Esse projeto tramitou por 13 (treze) anos, recebeu substitutivos, posteriormente reuniu outros projetos que tratavam de temas semelhantes. Foi também apelidado de "AI-5 digital" e de "Lei Azeredo", eis que o político brasileiro Eduardo Azeredo foi o relator do Projeto em diversas fases e também um dos defensores da sua aprovação. Na justificativa do Projeto, consta: *Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Daí a necessidade de uma lei que defina os crimes cometidos na rede de informática e suas respectivas penas.*

O Projeto, que em sua redação original, em 1999, continha 18 artigos, converteu-se na Lei n. 12.735/2012, com apenas quatro artigos. De fato, sofreu forte rejeição da sociedade, ativistas e

pessoas que protestavam contra o possível vigilantismo e riscos de uma lei que poderia punir, segundo o ativismo, o “fato de ser internauta”. Não foi possível aprovar o Projeto de Lei n. 84/99 como desejado, tanto que se desmanchou, desfigurou-se absolutamente, eis que, ao ler a Lei n. 12.735/2012, não se imagina que tenha se originado do precitado projeto de lei.

Neste período, em que se discutia e não se chegava a um consenso sobre o Projeto de Lei n. 84/99, em uma guerra mais política do que técnica, de mais de uma década, um fato agravou o cenário nacional em meados de 2010 e 2011: os constantes ataques a *sites* governamentais e de políticos e a exposição de dados privados envolvendo pessoas públicas. De fato, vários grupos de ciberativistas começaram a atuar no Brasil, manifestando, invadindo e indisponibilizando serviços informáticos[46].

Entendeu-se que o Projeto de Lei n. 84/99 era inviável e não conseguiria ser aprovado. Foi então que, em uma espécie de “acordo”, foi proposto, em 29 de novembro de 2011, pelo Deputado Paulo Teixeira, o Projeto de Lei n. 2.793/2011, que dispunha sobre a tipificação criminal de delitos informáticos. Tratava-se de um projeto para fazer frente à proposta de criminalização trazida pelo Projeto de Lei n. 84/99, demasiada e desproporcional e que poderia criminalizar condutas corriqueiras no mundo da tecnologia da informação.

Considerou-se também um outro projeto de lei, pois o Projeto de Lei n. 84/99 não poderia mais ser modificado segundo os regimentos do Congresso Nacional. Deixava de lado o Projeto de Lei n. 2.793/2011 qualquer discussão sobre a guarda de *logs* (registros de conexão e/ou navegação) por parte de provedores de acesso e aplicações de Internet, ponto muito discutido e enfaticamente reprovado por parte da sociedade em inúmeros manifestos. Com isso, propunha-se um projeto mais “suave”, sem pontos polêmicos, de menor resistência social, que deveria ser submetido a ampla discussão e audiências públicas.

Não foi o que aconteceu, pois em 4 de maio de 2012, com o fato envolvendo a atriz Carolina Dieckmann, relativo ao suposto vazamento de fotos íntimas na Internet, diversos requerimentos de urgência foram apresentados em relação ao Projeto de Lei sob análise, que tramitou em tempo

recorde. Proposto em novembro de 2011, em novembro de 2012 o Projeto de Lei n. 2.793/2011 se transformava na Lei n. 12.737/2012, a conhecida "Lei Carolina Dieckmann", que aqui se nomina de "Lei de Crimes Informáticos". Uma derrota para os ativistas. Um avanço, ainda que modesto, para os que buscavam havia mais de uma década um marco mínimo em termos criminais.

Segundo a justificativa do Projeto, convertido na Lei n. 12.737/2012, *ainda, com relação ao PL 84/99, nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática – independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente – já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade de risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. Exemplo disso é a criação de um capítulo com o objetivo de tutelar juridicamente, como bem jurídico protegido, a "segurança dos sistemas informatizados". Tal estratégia, como já apontado, resulta na possibilidade de punição gravosa a meras condutas que, por sua natureza ou intenção, não mereceriam ensejar a repressão penal – como o acesso não autorizado a sistemas informáticos decorrentes de testes de segurança efetuados sem a prévia anuência dos titulares de sistemas informatizados.*

Neste cenário, estando as Leis n. 12.735 e n. 12.737, ambas de 2012, em vigor, desde abril de 2013, pode-se afirmar que o Brasil já conta com leis específicas de crimes cibernéticos, impulsionadas por um casuísmo, "populismo penal", e que, ainda que modestas, uma contendo apenas um comando e a outra contendo apenas um novo tipo penal e duas "atualizações tecnológicas" em tipos já existentes, pretendem auxiliar no combate ao crime cibernético, sem, contudo, desrespeitar direitos e garantias fundamentais. Mas a teoria nem sempre é o que se vê na prática e

não se pode deixar de consignar que os riscos que os legisladores apontavam no Projeto de Lei n. 84/99, grande parte, se fazem presentes na Lei n. 12.737/2012, como será visto nesta obra.

Em uma sociedade de risco, a aprovação de um Projeto de Lei às pressas, sem ampla discussão, pode gerar margens a enquadramentos errôneos e atitudes que violem direitos e garantias dos cidadãos. E é o que veremos no capítulo seguinte.

Assim, no Brasil, tínhamos somente a Lei n. 9.983/2000, que alterou o Código Penal, até a edição e publicação das Leis n.12.735/2012 e n. 12.737/2012. A Lei 12.737/2012 tipifica a invasão de dispositivo informático, a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e a falsificação de cartão de crédito ou débito. Nos próximos capítulos estudamos em detalhes as legislações.

No entanto, cabe mencionar, ainda, o disposto no art. 15 da Lei n. 6.996, de 7 de junho de 1982, que dispõe sobre a utilização do processamento eletrônico de dados nos serviços eleitorais e dá outras providências:

Art. 15: Incorrerá nas penas do art. 315 do Código Eleitoral quem, no processamento eletrônico das cédulas, alterar resultados, qualquer que seja o método utilizado.

Tal regramento, em vigor desde a década de 1980, especificamente na seara eleitoral, classifica como conduta criminosa a alteração de resultados no processamento eletrônico das cédulas, complementando o art. 315 do Código Eleitoral (Lei n. 4.737/96):

Art. 315. Alterar nos mapas ou nos boletins de apuração a votação obtida por qualquer candidato ou lançar nesses documentos votação que não corresponda às cédulas apuradas:

Pena – reclusão até 5 (cinco) anos e pagamento de 5 (cinco) a 15 (quinze) dias-multa.

6.9.15. Dados internacionais

A África é o continente com mais países sem leis específicas sobre crimes digitais. A América do Sul, Central e do Norte também se destacam por serem os continentes com menos países que possuem

leis de crimes informáticos ao lado da Oceania (onde somente Austrália e Nova Zelândia possuem legislação sobre o tema).

Ásia e Europa são os continentes com mais países com legislações e disposições envolvendo crimes informáticos. Europa é a campeã, até mesmo por força da Convenção de Budapeste. Na Europa, apenas Andorra, Macedônia, Bósnia e Herzegovina, Liechtenstein, Macedônia, Maldova, Mônaco, San Marino e Sérvia e Montenegro, até o fechamento desta edição, não contavam com legislação ou disposições sobre crimes informáticos. Importa dizer também que alguns países da União Europeia, como Ucrânia, assinaram a Convenção de Budapeste, mas ainda não aplicaram os conceitos na legislação para a Internet.

Importa dizer que a Rússia, por fim, não assinou a Convenção de Budapeste, que trata do combate ao cibercrime e a padronização das legislações dos Estados-membros. O país categoricamente não adota a Convenção de Budapeste, especialmente em relação ao art. 32, que trata do chamado "acesso transfronteiriço", que permite que as agências de inteligência de alguns países acessem as redes de computadores de outros países para realizar operações, sem o conhecimento das autoridades nacionais.

Países sem leis, como Serra Leoa, Senegal, Vietnã, Iêmen e Irã, podem ser utilizados por sistemas *proxies* de modo a facilitar acessos anônimos para práticas criminosas, sendo utilizados como técnicas antiforenses.

7.

LEI N. 12.735/2012 E SEUS VETOS

7.1. Trâmite legislativo e generalidades

A Lei n. 12.735/2012 adveio do Projeto de Lei n. 84/99 (89/2003) e promoveu alterações no Código Penal (Decreto-Lei n. 2.848, de 7-12-1940) e no Código Penal Militar (Lei n. 7.716, de 5-1-1989). A legislação, apesar de prever em seu preâmbulo que tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, contra sistemas informatizados e similares, na verdade não acrescentou tipo penal algum ao ordenamento jurídico.

A lei estabelece em seu art. 4º a possibilidade da polícia judiciária estruturar órgãos especializados no combate à ação delituosa em redes de computadores, dispositivos de comunicação ou sistemas informatizados. Nada fala em relação à cooperação da iniciativa privada, muito utilizada, por exemplo, nos Estados Unidos.

Nos termos do antigo "Substitutivo do Senado ao Projeto de Lei da Câmara n. 89, de 2003[47] (PL n. 84/99, na casa de origem), que pretendia alterar o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal e a Lei n. 9.296, de 24 de julho de 1996, e dar outras providências, tínhamos os seguintes conceitos para redes de computadores, dispositivos de comunicação ou sistemas informatizados, elencadas no então art. 16:

Dispositivos de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia.

Redes de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, nacional ou mundial através dos

quais é possível trocar dados e informações.

Sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente.

A Lei n. 12.735/2012 alterou o inciso II do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989 (que define os crimes resultantes de preconceito de raça e cor) para fazer prever a possibilidade da cessação das transmissões eletrônicas ou publicação em qualquer meio, em casos de fabricação, comercialização, distribuição ou veiculação de símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo, especificamente, quando houver a utilização dos meios de comunicação social ou publicação de qualquer natureza.

Estas são as disposições trazidas pela Lei n. 12.735/2012:

Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Como visto acima, foi promovida uma alteração no inciso II do § 3º do art. 20 da Lei n. 7.716, de 5 de janeiro de 1989, que passou a vigorar com a seguinte redação:

Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei n. 9.459, de 15/05/97)

Pena – reclusão de dois a cinco anos e multa.

(...)

§ 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência:

(...)

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

(...)

7.2. Vetos da Presidência da República

A Lei n. 12.735/2102 não foi aprovada sem reservas. Em verdade, a Presidência da República efetuou dois vetos no texto final que foi encaminhado pelo Congresso Nacional.

A mensagem de veto[48] parcial, por contrariedade ao interesse público, foi a de n. 525, de 30 de outubro de 2012, remetida ao Senado Federal pela Presidência da República, retirando a pretensa alteração do art. 298 do Código Penal, que equiparava o documento particular ao cartão de débito ou crédito, bem como removeu novas hipóteses de incidência do tipo penal "favor ao inimigo", relativas aos incisos II e III do art. 356 do Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar. Apresentamos na sequencia os detalhes sobre os vetos.

7.2.1. Falsificação de cartão de crédito

A legislação oriunda do Projeto de Lei n. 84/99 foi absolutamente desfigurada para que pudesse ser aprovada. Neste ponto, o Projeto de Lei também alterava e equiparava a documento particular o cartão de crédito e débito, inserindo um parágrafo único no art. 298 do Código Penal, que trata do crime de falsificação de documento particular.

Em verdade, a Lei n. 12.737 (que será estudada no próximo capítulo), também publicada em 30 de novembro de 2012, já fizera tal inserção, alterando o art. 298 do Código Penal.

Por isso, o veto, sob o fundamento *para garantir a coerência da legislação pátria e evitar a coexistência de dois tipos penais idênticos, dada a sanção do crime de falsificação de cartão, com* nomen juris *mais adequado, ocorrida nesta data.*

7.2.2. Crime de favor do inimigo

Outra alteração que o Projeto de Lei n. 84/99 promoveria era em relação ao Código Penal Militar (Decreto-Lei n. 1.001, de 21-10-1969), especificamente em relação ao art. 356, crime de favor do inimigo, assim transcrito:

Art. 356. Favorecer ou tentar o nacional favorecer o inimigo, prejudicar ou tentar prejudicar o bom êxito das operações militares, comprometer ou tentar comprometer a eficiência militar:

I – empreendendo ou deixando de empreender ação militar;

II – entregando ao inimigo ou expondo a perigo dessa consequência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões ou qualquer outro elemento de ação militar;

III – perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões ou qualquer outro elemento de ação militar;

IV – sacrificando ou expondo a perigo de sacrifício força militar;

V – abandonando posição ou deixando de cumprir missão ou ordem:

Pena – morte, grau máximo; reclusão, de 20 (vinte) anos, grau mínimo.

A alteração proposta seria especificamente em relação aos incisos II e III, que passariam a vigorar com a seguinte redação:

II – entregando ao inimigo ou expondo a perigo dessa consequência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III – perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.

De fato, a expressão “dado eletrônico” foi inserida nos incisos do tipo penal com o escopo de responsabilizar militares, que por ação ou omissão negligenciassem com tais dados relativos a

ações. A pena cominada era a de morte.

Tais alterações foram vetadas pela Presidência da República sob o fundamento de que *a amplitude do conceito de dado eletrônico como elemento de ação militar torna o tipo penal demasiado abrangente, inviabilizando a determinação exata de incidência da norma proibitiva.*

Estranha e diversamente, não entendeu a Presidência da República, no mesmo sentido, no caso do art. 154-A do Código Penal (acrescentado pela Lei n. 12.737/2012), que tipifica a invasão de dispositivo informático, eis que, neste tipo, a expressão "dado ou informação" também comporta uma amplitude conceitual, inviabilizando a determinação exata de incidência da norma proibitiva.

7.3. Tipos penais e disposições que não entraram

O Projeto de Lei n. 84, proposto em 24 de fevereiro de 1999 no Senado[49], era um projeto bem abrangente e com vários tipos informáticos. Foi alterado em 2008, com o substitutivo do Senado ao PLC 89/2003[50] (número que recebeu na Câmara). Assim, o Projeto de Lei n. 84/99 foi substituído pelo PLC 89/2003, que, posteriormente, retornou a ser o Projeto de Lei n. 84[51].

Durante este trâmite de mais de 12 (doze) anos, o Projeto de Lei n. 84/99 contemplou diversos tipos penais, que aos poucos foram se alterando em alguns termos, até que foram suprimidos. Não é pretensão deste livro estudá-los, pois não estão em vigor, mas apresentamos os principais tipos penais existentes e que não prosperaram na Lei n. 12.735/2012 (tipos podem conter alguma pequena variação de termos, considerando que durante anos sofreram várias alterações, até que, por fim, foram eliminados do último substitutivo que se transformou na lei).

7.3.1. Acesso não autorizado à rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso.

A pena proposta era de reclusão, de 1 (um) a 3 (três) anos, e multa.

Tipo semelhante foi aprovado com a edição da Lei n. 12.737/2012, sendo previsto no art. 154-A do Código Penal, que trata do acesso indevido a dispositivo informático.

7.3.2. Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível.

A pena proposta era de reclusão, de 1 (um) a 3 (três) anos, e multa.

Tipo retirado do Projeto n. 84/99 por ser muito amplo e comportar extensiva interpretação, como, por exemplo, a possibilidade de punição daquele que, sem desejar ou solicitar, recebesse por *e-mail* ou outra forma tecnológica, de alguém, contendo conteúdo protegido por direitos autorais.

7.3.3. Divulgação ou utilização indevida de informações e dados pessoais

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

A pena proposta era de detenção, de 1 (um) a 2 (dois) anos, e multa.

Tipo que visava proteger os dados pessoais das manipulações e tratamentos indevidos. Tal delito fora removido também por força da discussão que existe no Brasil sobre o anteprojeto de proteção de dados pessoais, que traz disposições semelhantes e que imprescinde de maiores debates[52].

7.3.4. Dano informático

O art. 163 do Código Penal ficaria com a seguinte redação: *Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio,* mantendo-se a mesma pena de detenção, de um a seis meses, ou multa.

Tal delito não foi aprovado. Para parte da doutrina, as novas disposições trazidas pelo art. 154-A da Lei 12.737/2012 contemplam em parte os casos em que da invasão decorre dano informático. Para outra corrente, o crime de dano, mesmo sem a expressão "dado eletrônico alheio" em seu tipo, aplica-se aos casos que o agente destrói dados ou informações eletrônicas, como, por exemplo, por meio de um vírus informático.

Para Daniel Zaclis (2007, p. 1), a ânsia legislativa levou o então legislador do Projeto de Lei n. 84/99 a tentar prever o dano informático, porém este é desnecessário, pois a doutrina compreende coisa como aquilo que possui valor econômico, logo, *software* e sistemas informáticos podem sofrer danos, cujos autores podem ser punidos nos termos do art. 163 do Código Penal.

Para o referido autor, "não se deve permitir que a rapidez com que aparecem as novas tecnologias nos faça intensificar as ações legislativas sem antes atentarmos às leis já existentes. E, quando se fala em vírus informático, tem-se a possibilidade de aplicação do art. 163 do Código Penal" (ZACLIS, 2007, p. 2).

7.3.5. Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.

A pena proposta seria reclusão, de 1 (um) a 3 (três) anos, e multa.

O tipo penal previa a punição pela mera inserção ou difusão de código malicioso em dispositivo computacional. Tratava-se de alto subjetivismo interpretativo, o que poderia conduzir a erros graves. Não existe uma definição de código malicioso clara.

Igualmente, a simples "difusão do código", sem que dano algum ocorresse, era ponto da legislação

que gerou grande rejeição de parte da sociedade.

7.3.6. Inserção ou difusão de código malicioso seguido de dano

O art. 163-A teria um parágrafo qualificador, no seguinte sentido*: Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado.*

A pena era de reclusão, de 2 (dois) a 4 (quatro) anos, e multa. Tal dispositivo também não prosperou.

7.3.7. Estelionato eletrônico

O delito de estelionato, previsto no art. 171 do Código Penal, também seria alterado, para inserir uma disposição relativa àquele que difundisse, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. A pena seria a mesma do *caput*.

Igualmente, se o agente se valesse de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena seria aumentada de sexta parte.

7.3.8. Atentado contra a segurança de serviço de utilidade pública

Buscava o legislador inserir o serviço de informação e comunicação dentre aqueles passíveis de sofrer atentado contra a segurança, com a alteração do tipo previsto no Código Penal, que ficaria assim redigido:

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Essa alteração não prosperou e a expressão "informação ou telecomunicação" não consta no atual art. 265 do Código Penal.

7.3.9. Falsificação de dado eletrônico ou documento público

Este tipo penal também foi removido do último substitutivo, que resultou da Lei n. 12.735/2012. Alterava o art. 297 do Código Penal, que passaria a vigorar com a seguinte redação:

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:

Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

Como não prosperou, o art. 297 permanece no Código Penal, porém sem a expressão "dado eletrônico".

7.3.10. Pornografia infantil informática

O Projeto de Lei n. 84/99 pretendia trazer penas mais severas para o delito de pornografia infantil, com disposição expressa em seu art. 20. Ademais, era objetivo incluir no rol de competências legais da Polícia Federal "delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado".

Em meio ao trâmite do Projeto de Lei n. 84/99, a Lei n. 11.829/2008 alterou o Estatuto da Criança e do Adolescente, fazendo prever completas disposições sobre pornografia infantil na Internet[53].

Igualmente, não prosperou a disposição do art. 21 do Projeto de Lei n. 84/99, que pretendia ampliar a competência da Polícia Federal, por evidente quebra do pacto federativo contemplado na Constituição Federal, pois neste caso todas as infrações tratadas no Projeto seriam de competência da Justiça Federal.

Certamente, a Justiça Federal e a Polícia Federal não teriam condições de absorver tamanha demanda.

7.3.11. Guarda de **logs** *e obrigações para os provedores de serviços e de acesso à Internet no Brasil*

O Projeto de Lei n. 84/99, hoje Lei n. 12.735/2012, trazia em seu art. 22 obrigações para provedores do serviço de acesso à Internet no Brasil.

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, bem como os prestadores de serviço de conteúdo, são obrigados a:

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e o Ministério Público mediante requisição;

II – preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – informar, de maneira sigilosa, à autoridade policial ou judicial, informação em seu poder ou que tenha conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas, autoras, coautoras ou participes do mesmo fato.

Essa disposição, sem dúvida, era uma das mais polêmicas. Obrigava provedores de acesso a guardar registros de conexão por três anos, permitia que autoridades investigatórias (Polícia e Ministério Público) acessassem tais dados, sem necessidade de ordem judicial e, principalmente,

criava a figura do apelidado "provedor dedo-duro", que deveria informar a polícia ou o judiciário sempre que identificasse informações que revelassem indícios da prática de crime[54].

O art. 22 foi retirado do Projeto de Lei n. 84/99, antes da sua conversão na Lei n. 12.735/2012. Tal fato se deve também à discussão do Marco Civil da Internet, a chamada "Constituição da Internet", Projeto de Lei n. 2.126/2011 e hoje Lei n. 12.965/2014, e que concentra obrigatoriedade dos provedores de conexão em guardarem os registros de conexão por 1 (um) ano e dos provedores de aplicações, em guardarem os registros de acesso a aplicações por 6 (seis) meses. Vejamos:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Do mesmo modo, pelo Marco Civil da Internet, não existe mais o "provedor dedo-duro", sendo que o provedor de Internet só será responsabilizado pelo conteúdo de terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.

8.

LEI N. 12.737/2012 E OS CRIMES INFORMÁTICOS

A Lei n. 12.737/2012, conhecida como "Lei Carolina Dieckmann", oriunda do Projeto de Lei n. 2.793/2011, ao contrário da Lei n. 12.735/2012, traz novos tipos penais e algumas alterações legislativas relevantes. No presente capítulo, analisamos todos os pontos e detalhes da nova legislação.

8.1. Trâmite legislativo e generalidades

A criminalização dos abusos do domínio da informática sempre foi objeto de controvérsias. Não restam dúvidas que a ausência de leis específicas, somada a ultrapassadas práticas investigativas, era (ou é) elemento que influenciava o criminoso digital no seu intento, amparado por quatro paredes e o suposto anonimato proporcionado pelo seu computador.

Milhões de pessoas lidando com tecnologia da informação, sem conhecerem os riscos e os crimes cibernéticos. Pesquisa publicada em 2012 dá conta de que 30% dos internautas do mundo não se importavam com o crime virtual[55]. Nesse sentido, o ambiente, no Brasil, sempre foi propício para *crackers* (criminosos digitais), que viam um verdadeiro *playground* cibernético se moldando no horizonte.

Em que pese existirem tipos penais que possam criminalizar aquele que adultera ou destrói dados informatizados (art. 163 do Código Penal), ou mesmo aquele que copia ou move indevidamente informações (art. 155 do Código Penal) é inegável que tais "enquadramentos forçosos" sempre foram objeto de muitos e acalorados debates sob o prisma da "analogia *in malan partem*" e do princípio da reserva legal.

Para muitos doutrinadores, dados ou informações não poderiam ser subtraídos, diga-se, saírem da esfera de disponibilidade da vítima, nem mesmo ser objeto de destruição (considerando que comumente dados são copiados indevidamente). Para outros, ainda que intangíveis, dados, por terem relevância econômica, tal como a energia elétrica[56], mereciam a relevância do ordenamento jurídico penal[57].

Não obstante, no que tange ao delito de acesso indevido a dispositivo informático, a Lei n. 12.737/2012 longe está de apaziguar a questão acima mencionada, isto porque a punição é para a invasão (com finalidade dolosa), pouco importando o resultado desta atividade ilícita e não autorizada.

O tipo mais polêmico trazido com a Lei n. 12.737/2012, invasão de dispositivo informático, representa um crime de perigo abstrato, onde não se espera a ocorrência de resultado, forma legislativa que cresce diante do avanço da tecnologia e o temor do risco do seu uso indevido.

Assim, tem-se, segundo Bottini, "o que caracteriza a sociedade contemporânea não é o maior 'risco' existente, mas a ampliação da 'sensação de risco'. Os perigos que afligem a sociedade atual não são maiores do que aqueles que afetavam o cotidiano de nossos avós ou das gerações anteriores – talvez sejam até menores. Mas a 'vivência' destes riscos é mais presente. Seja pelas incertezas científicas sobre as técnicas e produtos que nos são ofertados diariamente, seja pela intensa cobertura feita pela mídia sobre acidentes e catástrofes, há uma sensação de insegurança maior, há um sentimento de proximidade do risco. Essa insegurança geral cria um discurso pela antecipação da tutela penal. A sociedade não admite mais aguardar a ocorrência de um resultado lesivo para aplicar uma pena. Há uma política de proibir comportamentos perigosos, mesmo que não causem resultado algum, como consequência desse clamor por maior segurança, maior tranquilidade, frente à nova sensação de riscos"[58].

Assim, na sociedade da informação, cada vez mais buscam-se proteger direitos supraindividuais, em um modelo preventivo do Estado contra os riscos e não contra ameaças concretas de lesão ao

bem jurídico protegido.

Em face do princípio constitucional da presunção de inocência, que não admite presunções contra o agente, entendemos que os delitos de perigo abstrato não encontram guarida em nossa legislação penal.

Consignamos, entretanto, que, em face de vivermos em um mundo de riscos, o legislador, valendo-se de todos os meios para prevenir e reprimir a criminalidade, tem se valido, cada vez mais, dos delitos de perigo abstrato, antecipando-se à produção do resultado. Assim é que, na Alemanha, em um banco, a simples troca de dinheiro para adquirir a droga já constitui o crime de aquisição. Entre nós, diante da Lei dos Crimes Informáticos, a simples invasão de dispositivo informático já configura crime, independentemente do resultado visado pelo agente.

Apelidada de "Lei Carolina Dieckmann", a Lei n. 12.737/2012, que tipifica os crimes cibernéticos, adveio do Projeto de Lei n. 2.793/2011[59], sendo agilizado no início de 2013 pelo "casuísmo em que fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na Internet". Na verdade, a legislação veio atender a uma demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente "circunscrita", em comparação aos projetos sobre crimes cibernéticos que tramitavam no Congresso Nacional.

Entendeu-se em aprovar uma lei menor, com pontos menos polêmicos, a não ter nada regulamentando crimes cibernéticos, eis que, diz o ditado, a lei é como remédio, deve ser ministrado em doses, pois se ministrarmos tudo de uma vez, podemos matar o paciente.

Passemos então à análise dos tipos penais trazidos pela Lei de Crimes Informáticos.

8.2. Invasão de dispositivo informático

8.2.1. Conceito

A cópia indevida de dados ou informações no Brasil era conduta sem tipo associado. Muitos promotores, em tais casos, ofereciam denúncias em face do crime de furto, previsto no art. 155 do Código Penal (subtrair, para si ou para outrem, coisa alheia móvel). Na doutrina, muitos asseveravam ser impossível a aplicação do tipo, considerando que a coisa "dados" não saía da esfera de disponibilidade da vítima, mas tão somente era "copiada". Um *"ctrl+c"* não poderia ser considerado furto. Estes ajustes na legislação criminal são supridos com a Lei n. 12.737/2012, pelo art. 154-A do Código Penal[60].

Na sociedade contemporânea, cada vez mais dependente de tecnologia da informação, é impossível se cogitar uma pessoa física ou jurídica que não interaja com pelo menos um dispositivo informático. Grande parte da população possui telefones celulares. Existem no Brasil mais de 250 milhões de aparelhos celulares[61].

Tokens, GPSs, *Tablets*, dentre outros, são exemplos de dispositivos informáticos. Ao contrário das inúmeras versões do Projeto de Lei n. 84/99 (Azeredo) e de outros Projetos que tramitaram no Congresso Nacional, onde tipos penais puniam a invasão a "rede de computadores" e "sistemas informáticos", quis o legislador do Projeto de Lei n. 2.793/2011 resumir o objeto ou foco da invasão a "dispositivo informático".

As expressões "redes de computadores" e "sistemas informáticos" comportavam várias interpretações que não pacificariam os entendimentos. Não se cogita da invasão de redes de computadores sem que também haja acesso a um dispositivo informático, e mais, caso se invadissem dispositivos informáticos em modo *off-line*, o fato seria atípico (se considerássemos a expressão "redes de computadores").

Por sua vez, ao prever a invasão a "sistema informatizado", a lei excluiria do tipo a invasão a dispositivos de armazenamento onde não existe um *soft-ware*, aplicativo, utilitário ou mesmo um *firmware* instalado, um sistema. Daí então a redução, especificação do objeto do tipo a "dispositivo informatizado". A lei pune quem invade dispositivo informatizado, pouco importando a existência ou

não de um "sistema informatizado".

Importante advertir que a Convenção do Cibercrime, assinada em Budapeste, classifica "sistema informático" como sendo "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles desenvolve, em execução de um programa, tratamento automatizado de dados".

Não temos um glossário na Lei n. 12.737/2012, o que pode gerar interpretações distintas para o termo "dispositivo informatizado". Invadir é devassar, ato ou ação de acessar indevidamente, mas à força, irrupção. Entrar em certo lugar e ocupá-lo pela força ou tomar, conquistar, na linguagem técnica, *ownar* (tomar a propriedade) ou realizar um *takeover.* Na sociedade da informação, dispositivo informático é todo o dispositivo capaz de tratar informação, diga-se, armazenar ou processar dados (cálculo, alteração, inclusão ou exclusão).

Qualquer interação de um indivíduo com um sistema informático é um acesso. A leitura de uma informação em um *display* de um celular ou em um monitor de um computador é um acesso. Acessar é "ter contato". Acessar indevidamente é acessar sem permissão, porém, acessar indevidamente não é invasão, já que, para que haja invasão, faz-se necessária a entrada forçada (ou, para alguns, embora não concordemos, uma forma não convencional de acesso). Logo, nem todo acesso indevido será considerado invasão.

Pessoas físicas ou jurídicas têm o direito à intimidade e privacidade, à segurança da informação, e este direito se estende ao que se encontra em seus dispositivos informáticos. Daí por que a Lei n. 12.737/2012 exige que mantenhamos incólumes tais dispositivos informáticos, sobretudo seu conteúdo, por meio do tipo penal que é inserido no Decreto-Lei n. 2.848/40 dentre os crimes contra a liberdade individual, a seguir citado:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou

instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I – Presidente da República, governadores e prefeitos;

II – Presidente do Supremo Tribunal Federal;

III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

8.2.2. Objetividade jurídica

No delito, em tela, protege-se a liberdade individual, o direito à intimidade e a segurança da informação, considerando que o objetivo é proteger dados e informações pertencentes a determinada pessoa. Para Márcio André Lopes Cavalcante (2013, p. 1), "o bem jurídico protegido é a

privacidade, gênero do qual são espécies a intimidade e a vida privada".

Tutela-se a liberdade individual de manter íntegros os dados dispostos em preceito informático, bem como ilesos os próprios dispositivos em si, protegidos por mecanismo de segurança (a lei não esclarece o nível ou o tipo de segurança), de acessos não autorizados, expressa ou tacitamente, com a finalidade de:

a) obter dados (objeto da alteração);

b) alterar dados;

c) destruir dados;

d) instalar vulnerabilidade para obter vantagem ilícita.

A lei estabelece, como condição para a prática do delito, que o dispositivo invadido esteja protegido por "mecanismo de segurança", não estabelecendo, pois (nem deveria), quais mecanismos são considerados seguros e se tal proteção é lógica (*software*), física (travas), dentre outras.

Para alguns juristas, um *modem* recém-adquirido, cuja senha padrão é "admin" ou "123mudar" para todos os equipamentos daquele fabricante, violado, em que pese apresentasse "mecanismo de segurança", não apresentava mecanismo eficaz, que sequer poderia ser considerado "proteção" (o dispositivo estaria praticamente aberto). A ausência de mecanismo de segurança conduz à atipicidade do fato. E sua ineficácia equivaleria à sua ausência. Esta corrente não é uníssona, pois existe corrente em sentido contrário, que advoga no sentido de que basta "mecanismo de segurança", pouco importando ser o mesmo eficaz ou não.

Não se confunda mecanismo de segurança com proteção contra gravação. O mecanismo de segurança deve ser considerado uma barreira entre o invasor e os dados ou informações armazenadas ou contidas no dispositivo. A proteção contra gravação apenas impediria a edição dos dados, não obstando o acesso a eles.

Um *pen drive* ou cartão de memória, aparentemente sem qualquer mecanismo para a proteção dos dados, que é subtraído pelo agente, que acessa os dados, copia-os indevidamente e depois os apaga.

Não haveria de se falar na incidência do crime ora em estudo, considerando que não houve "invasão", mas acesso a mecanismo desprotegido e destruição das informações (possivelmente, crime de dano, previsto no art. 163 do Código Penal). Poderia ainda o agente responder pelo furto do dispositivo (art. 155 do Código Penal).

Para parte da doutrina, no mesmo raciocínio, se o *pen drive*, sem qualquer mecanismo de segurança lógico (ou dentro do dispositivo), tivesse sido furtado de um cofre, estaria caracterizado o tipo comentado (Invasão de dispositivo informático – art. 154-A do Código Penal), considerando a existência de mecanismo de segurança físico (fora do dispositivo, mas que o protege). Importa dizer, o mecanismo de segurança não precisaria estar dentro do dispositivo, mas incidindo de alguma forma para a proteção do mesmo, ainda que proteção externa. Um *firewall* (*software* que protege ativos de acessos indevidos) que protege um dispositivo informático, a exemplo, pode estar instalado em um outro dispositivo. Seria forçoso não opinar pela existência de "mecanismo de segurança" neste caso, ainda que não instalado ou configurado diretamente no dispositivo invadido.

Ademais, desmerece ser confundida a invasão com a chamada "interceptação de dados ou telemática", realizada por programas como *Wireshark ou tcpdump*, já tipificada na Lei n. 9.296/96, em seu art. 10, onde o bem jurídico tutelado também são os dados, e onde se busca a proteção da transmissão e recepção dos precitados dados, coibindo-se o uso indevido ou não autorizado das informações.

Indaga-se: todo e qualquer "dado" poderia ser considerado um "dado informático"? O que seria dado informático, para efeito de incidência do novo delito em estudo (art. 154-A do Código Penal)? Qualquer representação de fatos pode ser considerada "dados". Embora o Projeto de Lei n. 89/2003, proposto pelo Senado, trouxesse, em seu art. 16, uma conceituação para "dados", importa relevar que tal artigo não entrou no projeto "resumido" que resultou na aprovação da Lei n. 12.735/2012.

Esta pode ser, no entanto, uma das interpretações para dados informáticos, sendo eles considerados *qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de*

processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado[62].

Discordamos desta interpretação. Dados só podem ser considerados informações quando adquirem significado. Se dados estão representando fatos, em tese, já seriam informações. De maneira que, segundo o conceito acima citado, poderíamos concluir que nem todos os dados estariam protegidos, mas apenas os que representam fatos, informações ou conceitos.

Mas qual seria a utilidade de se obter o nome de um banco de dados mediante técnica de *sql injection* (injeção de parâmetros para acesso a dados em um banco de dados)? Evidentemente, o valor se encontra nos registros, nas informações, no conteúdo do banco. Como inserido no tipo penal, o legislador tratou de proteger dados e não apenas informações (conjunto de dados em um contexto).

Para alguns juristas, é forçoso não admitir que o nome de um banco de dados possa ser considerado um dado e uma informação, embora seja dado aparentemente insignificante e que em tese não poderia causar dano ao titular de um sistema acaso descoberto (a menos que relacionado com outras informações). Em tese, ainda, para tal corrente, a descoberta do nome do banco não demonstraria a intenção de obter informações. Por outro lado, existem entendimentos contrários, no sentido de que toda e qualquer representação de fatos é dado, para a lei, pouco importando a "relevância" das informações obtidas. Para esta corrente, um *log* demonstrando que alguém conseguiu descobrir o nome de um banco de dados já seria uma contundente prova da intenção de obter dados, mediante invasão.

Temos, por exemplo, o agente que inicia a conduta de invasão e obtém somente o nome do banco de dados, sequer listando as tabelas e seus registros, não dando sequência, por sua vontade, no processo. Invadiu, mas aparentemente sem a intenção do tipo penal, simplesmente demonstrando a insegurança do sistema. Ora, o agente poderia obter a informação que quisesse, mas desligou-se do alvo. Como poderemos afirmar que tinha intenção de obter informações? Em outro exemplo, o agente que, mediante programa de *footprinting*, como *nmap*, descobre apenas informações do sistema

operacional do alvo. Haveria crime? Em nosso sentir, a lei não foi concebida para punir condutas desta natureza. De acordo com a teoria da imputação objetiva, seria o caso de ser aplicado o princípio da não incidência do âmbito de proteção da norma penal incriminadora, sendo atípico o fato.

Deste modo, sabemos que dados são elementos ou valores considerados discretos. Em outras palavras, dados são quaisquer registros associáveis a um evento ou ainda "informação não processada". Por sua vez, informação é o resultado do processamento, manipulação e organização dos dados, de forma que represente valor no conhecimento de quem a acessa.

Da mesma forma que humanamente e sem a ajuda de tecnologia é impossível ir de um lugar a outro sem caminhar, é impossível acessar um dispositivo informático sem obter dados, por mais inúteis e imprestáveis que possam parecer. Qualquer acesso, devido ou indevido, resulta em dados para o agente, ainda que esta não fosse sua intenção e ainda que o agente não perceba. Destaca-se, porém, que o tipo penal não exige a obtenção efetiva dos dados pelo agente, bastando o acesso com a finalidade de obtê-los (elemento subjetivo do tipo "com o fim de").

De modo que, presente o fim visado pelo agente, há crime ainda que não concretizada a finalidade. Logicamente que questões concretas deverão ser analisadas individualmente, pois a "necessária obtenção de dados" (muitos que não representam valor ou conhecimento ao invasor), sem a intenção do agente, para acesso a um dispositivo informático ou durante ou após uma invasão, não necessariamente pode ser considerada criminosa ou "intenção de obter dados ou informações relevantes sobre o alvo".

De outra ordem, necessário se faz refletir sobre a seguinte indagação: qual a quantidade de dados que um invasor poderia acessar para transformá-los em informação? Esta resposta não é pronta. Pode haver conhecimento em um único dado e pode não haver valor algum em *terabytes* de dados. O legislador não quis dar margem a esta discussão, punindo o acesso com o objetivo de obter dados, sejam eles quais forem, de qualquer importância, de qualquer valor, estruturados ou não.

Caberá ao Judiciário operar a justiça onde só existe a lei.

Em nosso sentir, porém, a caracterização ou constatação de que dados já reúnem elementos informacionais (ou que são dados obtidos automaticamente pelos sistemas e sem relevância alguma) deverá ser realizada mediante nomeação de perícia técnica (podendo ser a prova da intenção do agente). Assim a perícia computacional será indispensável e poderá representar a condenação ou absolvição de envolvidos.

8.2.3. Classificação criminal

Indaga-se na doutrina se o delito de invasão de dispositivo informático poderia se enquadrar no conceito de crime permanente, quando a consumação se prolonga no tempo. Embora o acesso indevido possa perdurar no tempo, fato é que consumada a conduta com a invasão, ainda que o agente imediatamente se desconecte do sistema invadido, estará caracterizada a conduta. Trata-se, pois, de crime instantâneo, já que a consumação ocorre no momento da invasão, ainda que o agente permaneça conectado ao sistema, pois em verdade não está "invadindo" o mesmo, que já se encontra "invadido", devassado.

Classifica-se também o crime de invasão de dispositivo informático como delito de fato permanente, na medida em que se exige o exame de corpo de delito, considerando que a invasão deixa vestígios. Assim, nos termos do art. 158 do Código de Processo Penal, *quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.*

Indaga-se: o agente responsável por um sistema computacional que negligencia e permite a invasão do mesmo, poderia responder pelo crime do art. 154-A do Código Penal? É o delito considerado **crime comissivo**, que exige uma ação positiva do agente, porém não podendo excluir uma conduta omissiva que auxilie outra comissiva (a este respeito, citam-se os exemplos de crimes informáticos cometidos por funcionários públicos, previstos nos arts. 313-A e 313-B do Código Penal, e que

também podem se dar de forma omissiva). Nestes crimes, o partícipe somente responde por eles se também agiu dolosamente. A culpa não é típica.

Temos o exemplo do colaborador que, em uma noite, desabilita o *firewall* ou o monitoramento do sistema, ou mesmo não aciona proteção do banco de dados, permitindo o acesso de *cracker*. Quem, de qualquer modo, concorre para o crime, incide nas penas deste, na medida da sua culpabilidade. De ver-se, entretanto, que não há participação culposa em crime doloso. De modo que o concorrente só será punido nos termos do art. 154-A do Código Penal quando agir dolosamente e não por ser incompetente.

A invasão de dispositivo informático é crime unissubjetivo, diga-se, pode ser praticado por uma só pessoa, embora nada impeça a coautoria ou participação. Deve-se considerar também a progressão criminosa no crime de invasão de dispositivo informático, diga-se, uma pluralidade de condutas delitivas encadeadas por uma sequência causal e certa unidade de contexto.

Normalmente, o agente invade com uma finalidade e o ato não para na invasão. Da invasão, pode o agente praticar outros crimes, como a extorsão (como nos casos de *ransonware*[63]), o estelionato, a difamação, o dano, dentre outros. Nestes casos, sempre que o antefato (*antefactum*) invasão for menos grave que o pós-fato (*posfactum*), o autor deverá ser punido somente pelo crime mais grave.

Pode ser considerado, o novo delito do art. 154-A do Código Penal, em determinados casos concretos, crime exaurido, diga-se, onde após a consumação, o agente leva o delito a outras consequências lesivas.

A obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo informático (por exemplo, instalando uma *botnet* ou *shell* na máquina da vítima), exaure o delito que se consumara com a invasão de dispositivo informático alheio.

Diga-se, o crime em si é formal (embora alguns autores sustentem ser material) e eventualmente poderá ocorrer o exaurimento. Pode ocorrer que, consumado o delito, a pena seja agravada por

incidência de causas de aumento de pena, segundo os §§ 2º e 4º, ou pode ocorrer delito mais grave (§ 3º), todos do art. 154-A do Código Penal.

Trata-se de crime de ação única, por possuir somente o verbo "invadir", que constitui o núcleo da figura típica.

Como mencionado, autores divergem se o crime é formal ou material. Para parte da doutrina, o crime é formal, se consumando mesmo sem a obtenção, adulteração ou destruição de dados. Para outra corrente o crime é material, pois exige um resultado para se consumar, pois não existe invasão sem acesso ao menos de leitura aos dados (VIANNA e MACHADO, 2013, p. 98).

Em nosso sentir, é crime formal, eis que, muito embora o tipo traga qual deve ser a finalidade do agente na invasão, não exige que tal finalidade seja atingida para a consumação. Basta a invasão, pouco importando o resultado. Ademais, é possível, sim, invadir, e retornar para o agente invasor apenas um cursor na *shell* do computador invadido (tela de terminal), momento em que, ainda não disparando nenhum comando, não leu o invasor dado algum.

É, pois, crime simples, não encerrando dois ou mais tipos em uma única descrição. É crime comum, pois pode ser praticado por qualquer pessoa, e também crime principal, na medida em que independe da prática de delito anterior, embora possa existir crime prévio à invasão, como o estelionato.

Pode também haver situações em que o fato seja crime putativo, quando o agente pressupõe que está realizando uma conduta típica, como a invasão, mas na verdade o fato não constitui crime, como, por exemplo, o acesso a dispositivo desprotegido ou possuindo o agente autorização para acesso ao mesmo. No mesmo exemplo, poderá haver situações em que se caracterize o crime impossível, tendo em vista a impropriedade do objeto, eis que, tal como não se mata um morto, não se invade o que está aberto. Até mesmo pela ineficácia do meio, o crime impossível poderá ocorrer, como no caso do agente que tenta invadir um sistema bancário com um *software* absolutamente ineficaz, comprovado por perícia técnica.

Igualmente, trata-se de crime doloso, exigindo que o agente realize a ação voluntária e consciente no que tange à conduta e ao resultado. A ação (invadir) não pode ser compreendida sem a vontade do agente (interesse em invadir um dispositivo informático).

Para que haja incidência do tipo previsto no art. 154-A do Código Penal, é preciso ainda ter consciência do fato e todos os seus elementos típicos, diga-se, elemento subjetivo do tipo (a invasão deve ocorrer com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita). Entenda-se por titular do dispositivo não apenas o proprietário, mas aquele que loca o dispositivo ou por contrato tem sua administração.

O dolo inclui, portanto, no crime de invasão, o objetivo que o agente queria alcançar. A invasão, fora desta realidade, é considerada fato atípico. Toda a invasão será investigada e a finalidade apurada em inquérito ou na instrução. Deve-se sempre considerar a finalidade do agente invasor.

Pode-se cogitar também do dolo eventual, onde o agente não queria o resultado, mas assumiu o risco de produzi-lo, como no exemplo de uma invasão onde o agente buscava identificar uma vulnerabilidade, porém, sem saber, acaba adulterando ou destruindo dados do sistema invadido.

Importa dizer, pode ocorrer também o chamado crime provocado, mediante flagrante preparado ou não, onde o agente é induzido à prática do crime por terceiro, como, por exemplo, na criação, comum em segurança da informação, de sistemas *Honeypot*, atrativos a invasores, e que chamam a atenção destes. Nestes casos, poderá ocorrer a não existência de crime, eis se tratar de crime impossível (art. 17 do CP).

Honeypots são criados como uma forma de atrair *crackers* para um sistema de rede, para que possa estudar o comportamento do atacante. Atraindo atacantes, é possível descobrir vulnerabilidades e aprimorar a segurança. Um agente que é identificado acessando um ativo dessa natureza, em tese, não pode responder por invasão de dispositivo informático, sobretudo se se tratar de um *Honeypot* de pesquisa.

8.2.4. Sujeito ativo

Qualquer pessoa pode praticar o crime em estudo. Empregados, terceirizados e estagiários podem praticar o delito em face da empresa em que laborem, desde que não tenham autorização para acesso ao dispositivo informatizado. Não pratica invasão, evidentemente, o legítimo usuário com credenciais para acesso, que obtém dados, os altera ou destrói, neste caso, podendo constituir crime de dano, previsto no art. 163 do Código Penal, ou mesmo crime da Lei n. 9.983/2000, que estabelece o "peculato informático", específico para funcionários públicos (arts. 313-A e 313-B do Código Penal).

Podem ocorrer casos em que o agente tinha acesso permitido ao dispositivo (*login* de rede), mas no sistema nele instalado (um ERP – sistema integrado de gestão empresarial, serviço de *e-mail*, por exemplo) tinha permissões restritas. Caso consiga violar suas permissões e tendo acesso a outras informações, poderia ser punido pelo art. 154-A? A lei é omissa, considerando que pune a invasão a dispositivo e não a sistema informatizado. Logo, o Judiciário deverá se manifestar diante dos casos concretos. Para nós, o fato é atípico diante do art. 154-A do Código Penal.

Alguns casos recentes, entretanto, podem apresentar um entendimento doutrinário, como no caso do aplicativo "Rastreador de Namorado" que era disponibilizado na loja do Google, tendo sido, posteriormente, removido[64]. A instalação do aplicativo sem autorização do dono do celular poderia ser enquadrada no conceito dado pela Lei n. 12.737/2012 ao art. 154-A.

Devem-se mencionar situações em que a invasão se dê pelo próprio provedor de acesso (que provê conexão à Internet), ou pelo provedor de conteúdo (que oferece serviços na Internet). O usuário, no Brasil, nunca sabe o que existe dentro dos códigos das aplicações disponibilizadas por tais provedores, bem como se estes de alguma forma procedem com acesso indevido aos dados dos mesmos.

Ainda, provedores podem ser coniventes com determinados criminosos digitais ou até mesmo cúmplices, como no caso em que a pessoa avisa que está sendo vítima de tentativas de invasão por

parte de um cliente de determinado provedor e este nada faz. A título ilustrativo, a Diretiva n. 2000/31/CE do Parlamento Europeu esclarece que provedores só podem ser considerados responsabilizados se tiveram conhecimento do conteúdo armazenado em seus servidores.

Nestas situações, indaga-se: o provedor poderia ser sujeito ativo de um crime digital, em modalidades omissivas ou comissivas? Denota-se a clara necessidade de uma melhor regulamentação envolvendo as responsabilidades dos provedores de acesso e conteúdo, que, talvez, possa derivar da interpretação e regulamentação da Lei n. 12.965/2014 (Marco Civil da Internet).

Até mesmo porque o art. 12 da Convenção do Cibercrime de Budapeste sugestiona a possibilidade de pessoas jurídicas serem responsabilizadas. Ademais, no âmbito internacional, alguns países efetivamente permitem a responsabilização da pessoa jurídica, como Portugal[65].

8.2.4.1. Fato realizado pela polícia: atipicidade

Não comete o crime a autoridade policial que apreende, mediante ordem judicial, aparelhos informáticos e manda periciar seus conteúdos para apuração criminal. Nestes casos, normalmente a polícia utilizará uma medida de contrassenha com ferramentas como *John the Ripper, Cain* ou *Ophcrack* para acessar o disco ou o sistema operacional protegido por senha. Tais condutas, nem por aproximação, poderão ser consideradas criminosas.

Sob outro aspecto, qualquer ação policial sem um mandado judicial, por lógica, será considerada criminosa, podendo os agentes incidir nas penas do delito previsto no art. 154-A do Código Penal.

8.2.5. Sujeito passivo

Em tese, sujeito passivo do delito seria a pessoa física ou jurídica que tem a propriedade do dispositivo informático. A nosso sentir, tal rol deve ser ampliado. Hodiernamente muitos titulares de dados ou informações locam ou contratam provedores de armazenamento, hospedagem, *co-location* ou *cloud computing* para o tratamento de seus dados. Pesquisas revelam que no Brasil 75% das

grandes empresas já utilizam recursos de computação *nas nuvens,* onde os dados não se encontram hospedados nos ativos e *hardwares* na própria empresa, mas em serviços de terceiros. Estimativas indicam que, em 2015, 41% das empresas[66] utilizarão serviços *nas nuvens.*

Somam-se a esses fatos novos conceitos, como o *Bring Your Own Device* (BYOD), em que colaboradores usam seus próprios dispositivos (de sua propriedade) nas empresas que laboram, processando dados corporativos.

Indaga-se, se com a computação "da nuvem" ou BYOD, e outras tecnologias que surjam, ao se invadir dispositivo que não pertence à vítima, mas tão somente locado por esta ou processando dados desta, se a mesma poderia ser sujeito passivo do crime.

Segundo parte da doutrina que já se pronunciou sobre o tema, é atípica a conduta do empregador que acessa *e-mails* pessoais do empregado, sem sua autorização, armazenados em seu computador de trabalho (VIANA e MACHADO, 2013, p. 94). Isto porque o legislador errou ao proteger apenas o titular do dispositivo informático, não estendendo tal proteção ao titular dos dados. Assim, se invado dispositivo informático próprio e lá acesso indevidamente informações de terceiros, em tese não haverá crime.

Em nosso entendimento, sujeito passivo pode ser o titular dos dados, armazenados em dispositivo informático, e não somente o titular do dispositivo em si. Pode ser que o titular do dispositivo sequer tenha interesse em perseguir criminalmente o invasor de um de seus dispositivos alocados para clientes. A exemplo, um provedor de hospedagem, que vê um de seus clientes invadidos.

Se o titular do dispositivo tem legitimidade passiva no crime, não é coerente que se afaste da legitimidade o titular dos dados armazenados no dispositivo.

Destaque-se, outrossim, que maridos, esposas, noivos, noivas ou namorados poderão ser vítimas do crime em estudo praticado pelos seus parceiros, quando estes acessarem indevidamente seus dispositivos, considerando que a relação de namoro ou matrimônio não pressupõe autorização expressa ou tácita para acesso aos dispositivos informáticos.

8.2.6. Tipo objetivo

O núcleo do tipo é invadir, ou seja, devassar dispositivo informático necessariamente alheio, protegido por mecanismo de segurança, com a intenção de obter, alterar, destruir dados ou instalar vulnerabilidade com finalidade de obter vantagem ilícita. A nosso sentir, um crime formal que não exige a produção do resultado para a consumação, ainda que possível que ele ocorra. Como já vimos, entendemos que invadir exige algo além do que acessar indevidamente.

Deste modo, basta a invasão com a intenção, para que a conduta do agente faça subsunção perfeita ao tipo penal. Pode-se indagar como a "prova da intenção" será feita ou colhida. Certamente, esta se dará diante do caso concreto e incluirá elementos que deverão ser analisados por Delegados, Investigadores, Peritos, Ministério Público e Juízes, incluindo, mas não se limitando a:

a) características do delito;

b) existência de dados da vítima no computador do agente invasor;

c) existência de *e-mails*, *chats*, *sites* ou provas que comprovem interesse na obtenção ou manipulação indevida de dados;

d) existência de provas eletrônicas que comprovem objetivo de vantagem ilícita ou vulnerabilidade instalada com esta finalidade;

e) registros e *logs* que comprovam a tentativa de listagem, cópia dos dados, alteração ou mesmo exclusão das informações/registros;

f) reincidência.

De ordem inversa, a não identificação de um dos elementos (rol meramente exemplificativo) acima pode resultar na conclusão que o agente não tinha o escopo malicioso, mas tão somente "bisbilhotava" conteúdo em dispositivo alheio. Um dos exemplos seria o caso em que o perito, analisando o código do *malware* ou *software* usado pelo agente, identifica que o *payload* do código não era malicioso, mas tão somente executava alguma função ou aplicativo no sistema, como exemplo, a calculadora. Note-se que pelo código é possível dimensionar qual era a intenção do

agente, claramente. É possível, via perícia forense computacional, identificar, por exemplo, se a intenção do agente era testar a segurança do sistema ou realmente obter dados.

A invasão deverá se dar mediante violação de mecanismo de segurança. O legislador só pune a invasão a dispositivo protegido. Em uma analogia, seria como se o legislador não punisse o furto de um carro que não possui alarme.

Questão que deverá ser enfrentada é se a invasão em que o agente não tenha intenção de copiar os dados, logo não demonstrando intenção na obtenção dos mesmos, mas tão somente os "exibe", "lista", diretamente na base de dados invadida, poderia ser considerada criminosa.

É sabido na comunidade técnica que programas podem interagir com bancos de dados por meio da linguagem SQL (*Structured Query Language*), Logo, agentes podem, em *sites* e serviços inseguros ou desprotegidos, disparar instruções que permitem desde a inclusão de registros (INSERT) à exclusão completa da tabela de dados (DROP TABLE). Neste cenário, uma simples instrução para listar os registros (SELECT) poderia ser considerada criminosa?

Parte da doutrina especializada, mais afeta à área técnica, entende que na listagem ou *select* não existe a obtenção de dados (DUMP), que pressupõe cópia, posse, transmissão, logo, não reunidos os elementos do tipo penal na mera listagem de registros de uma tabela executada diretamente na vítima. Alguém que dispara instrução para listar os dados de uma tabela da vítima, remotamente, não demonstra, para esta corrente, a intenção de obter os dados. Em verdade, está testando, listando, avaliando a possibilidade de serem exibidos, em nenhum momento os copiando para disco rígido ou sequer externando essa intenção. Logo, segundo esta linha de entendimento, é preciso avaliar outros comandos e instruções executadas pelo agente, em perícia.

O entendimento não é pacífico, pois outra corrente se posiciona no sentido de que a listagem dos dados, ainda que não copiados para o computador, já estaria inserida no contexto de obtenção, considerando que o agente já teve contato, acesso, ainda que visual, com as informações. Para esta corrente "obter" é "ter contato". Exemplificando, ainda que humanamente impossível a um agente

realizar uma rotina para listar (*select*) os salários de todos os colaboradores de uma empresa, e decorar cada informação sem copiá-la, uma instrução *Select Max* poderia somar toda a folha de pagamento da empresa, resultando em um único dado (informação) de valor, simples de memorizar e que pode causar danos à empresa se divulgado.

De outra ordem, ainda, tem-se como consenso a parte dos pesquisadores de segurança da informação que, em uma invasão que decorra de um ataque de *SQL injection*, tais *sites* ou serviços que aceitam essas técnicas estariam desprotegidos. Ora, se estão desprotegidos não possuem "mecanismo de segurança" efetivo, logo, para tal corrente, a obtenção, manipulação, ou alteração de dados mediante exploração desta vulnerabilidade não poderia ser considerada conduta criminosa, pois, se está vulnerável, pressupõe-se que esteja ausente a segurança.

Não é o que pensa a corrente formada por parte das autoridades policiais e judiciárias. A questão é polêmica, porém, sabe-se que vulnerabilidade é a falha ou a ausência de mecanismo de segurança. Para outros autores, a lei, entretanto, não exige que o mecanismo de segurança não falhe para proteger a vítima da invasão. Em nossa opinião, se o dispositivo informático estava comprovadamente vulnerável, diante da ação específica do agente invasor, não se pode negar que possuía mecanismo de segurança, mas falho, o que pode ser levado em consideração como circunstância na análise do crime.

Releva notar, outrossim, o entendimento existente de que o legislador não fez prever a punição para aquele que invade com a finalidade de inserir dados (INSERT), punindo aquele que obtém, deleta ou altera informações, logo, não caracterizando a inserção mecanismo para obtenção de vantagem ilícita (como, por exemplo, em caso que o agente insere seus dados em banco de dados de pessoas que recebem auxílio de determinado projeto do Governo), caracterizada por perícia, tem-se, em tese, como atípico tal fato. Para outra corrente, a intenção de inserção de dados poderia ser considerada intenção de "adulteração ou alteração da informação", logo, incidindo-se o art. 154-A do CP, como no caso do agente que invade e dispara comando para inserir um registro no banco, mas não consegue

por circunstâncias alheias à sua vontade, como, por exemplo, erro na instrução que tentou executar. Por outro lado, deve-se ponderar, nestes casos, se comprovada a inserção indevida, estará caracterizado o delito de falsidade ideológica, previsto no art. 299 do Código Penal.

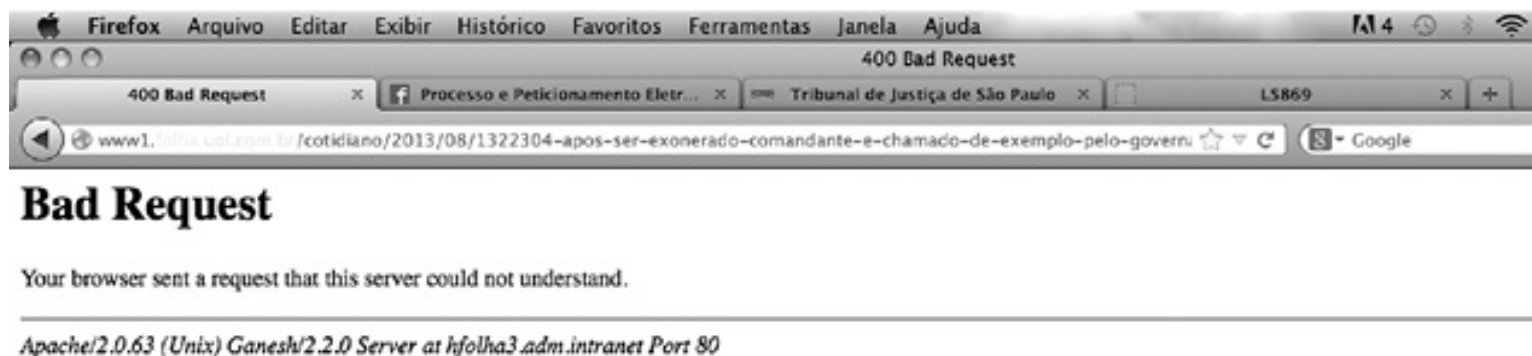
8.2.7. Tipo subjetivo

Inexistindo modalidade culposa prevista em lei, só se pune a modalidade dolosa do crime de invasão de dispositivo informático.

O dolo é a vontade livre e consciente de invadir o dispositivo. Já a expressão "para obter, adulterar, destruir informações, ou instalar vulnerabilidade para conseguir vantagem ilícita" configura um elemento subjetivo do tipo.

Como visto, existem elementos técnicos que podem ser verificados por autoridades na hora de concluir pela existência ou não de elemento subjetivo do tipo.

A invasão culposa tecnicamente pode ocorrer, por diversas formas, mas ela não será punida, como no caso do agente que, inexperiente e testando ferramenta de *pen test*, acaba por digitar um *host* alvo e acessá-lo, rompendo mecanismo de segurança (de forma automatizada) e recuperando dados do banco de dados.

De outra ordem, o agente que "tropeça na falha", obtendo dados, não pode, a nosso ver, ser punido por "invasão". A exemplo, aquele que, ao acessar um *site*, com erro, obtém um *Bad Request*, tendo acesso a dados do servidor *web*, como abaixo:

Embora tais informações obtidas possam ser úteis a um ataque, o agente as obteve sem qualquer

invasão (simplesmente pelo acesso ao *site*), ou intenção de obter, não podendo ser penalizado pela falha nos servidores da vítima.

A conduta será atípica sempre que a intenção do agente for jocosa, não agindo o mesmo com o fim de "obter, adulterar ou destruir dados ou informações".

8.2.8. Elemento normativo

Não ocorrerá o delito em se tratando de invasão de dispositivo próprio, como, por exemplo, no caso do destravamento ou *jailbreaking* de equipamento celular para funcionar com operadora distinta, realizado pelo próprio titular do dispositivo ou a mando deste. Por outro lado, a alteração de *soft-ware* de roteador para o chamado *"clone MAC"*[67], para que outro roteador ou *switch* possa distribuir o ponto de Internet, pode ser considerado crime de invasão, se o dispositivo está em comodato (porém poderá haver absorção por delito específico envolvendo telecomunicações). Neste sentido dispõe a Lei n. 9.472/97:

Art. 183. Desenvolver clandestinamente atividades de telecomunicação:

Pena – detenção de 2 (dois) a 4 (quatro) anos, aumentada da metade se houver dano a terceiro, e multa de R$ 10.000,00 (dez mil reais).

Parágrafo único. Incorre na mesma pena quem, direta ou indiretamente, concorrer para o crime.

A Justiça Federal já entendeu, no entanto, que o ato de compartilhar sinal de Internet não é crime[68].

Do mesmo modo, a alteração indevida de dados das *boxes* receptoras e *smartcards* de operadoras de telefonia, com fim de obtenção de sinal de TV a cabo, mesmo após a extinção do contrato, se o dispositivo estiver em comodato, pode ser considerada conduta criminosa[69].

Não ocorrerá o delito em casos de furto, roubo ou apropriação indébita de *token*, *On time password, SmartCards* ou outros dispositivos já configurados com senha ou chave privada (certificado digital) para acesso e autenticação em dispositivos ou sistemas informáticos (embora haja crime na conduta de se apropriar de tais dispositivos, não se pode falar em invasão em caso de

uso de tais “chaves” para abrir as portas dos dispositivos). Importa dizer, porém, que na maioria dos dispositivos existe a necessidade da digitação de um *pin* (senha) para uso da chave privada.

Assim, o chamado *password guessing* ou as tentativas de se acessar a senha de determinado dispositivo informático, se bem-sucedido, pode caracterizar o delito, se o agente tinha a intenção prevista no tipo do art. 154-A do Código Penal.

Estaremos, pois, diante de crime impossível por impropriedade do objeto, em casos de dispositivos desprotegidos, sem mecanismo de segurança, que são acessados indevidamente.

Não ocorrerá o delito diante da autorização expressa ou mesmo tácita do titular do dispositivo para acessar os dados. Na autorização expressa, o titular do dispositivo se manifesta autorizando o agente a acessar o sistema, ainda que indevidamente. Tais casos são muito comuns em tecnologia da informação e segurança de sistemas em testes de intrusão (*pentests*), análises de vulnerabilidades e ataques programados para se avaliar a maturidade de uma empresa em termos de segurança da informação.

O consentimento, ainda que tácito, do sujeito passivo torna o fato lícito, como, por exemplo, na hipótese em que é notificado, alertado ou comunicado pelo atacante de que este está a testar seus sistemas, ou que existem vulnerabilidades em seus ativos digitais, e não se manifesta a respeito se posicionando contra a conduta narrada.

Segundo Tulio Vianna e Felipe Machado (2013, p. 96), “a autorização tácita é aquela fornecida por atos que demonstrem inequivocamente a permissão do titular dos dados para que o agente os acesse. Como exemplo, pode-se citar o fornecimento de *login* de usuários e senha para um amigo. Ambos os tipos de autorização tornam a conduta atípica, mas a autorização tácita evidentemente exige uma prova em juízo mais complexa do que a simples apresentação de um documento”.

Em nossa ótica, o fornecimento de senha e *login* (desde que não sejam furtados tais dados) é nítida permissão de acesso, não havendo que se falar de invasão, considerando não existir mecanismo de segurança violado.

Mais uma vez a questão que se coloca é se o titular do dispositivo não for o titular dos dados. Como se avaliará eventual autorização expressa ou tácita para acesso aos sistemas? Somos adeptos do entendimento de que todos aqueles que possam sofrer danos com a invasão são legitimados a se manifestar no que tange à autorização para invasão do ativo, seja ele titular dos dados ou meramente titular do dispositivo que os armazena. Tal questão demandará revisão dos contratos entre prestadores de serviços de tecnologia da informação, hospedagem, *cloud*, prevendo questões de *data loss prevention* e SLA (*Service Level Agreements*).

A prestação de serviços *White hat*, desde que não ilegal, não se constitui em modalidade criminosa, sendo que o crime só é possível diante da invasão não autorizada ou mesmo do acesso não permitido.

Para alguns doutrinadores, o agente que tem uma senha não pressupõe necessariamente que tenha autorização, pois pode tê-la obtido mediante crime antecessor ou outra manobra. Logo, acessando com a senha o sistema, mas não tendo autorização, estaria acessando indevidamente e sem autorização. Por outro lado, acesso indevido não é invasão e neste cenário forçoso, em nossa visão, seria enquadrar o agente no delito do art. 154-A do Código Penal.

Já se a pessoa tem autorização para acesso e manipula indevidamente a base de dados, não há que se falar da aplicação do art. 154-A do Código Penal, valendo, em caso de sujeito ativo que seja funcionário público, o disposto no art. 313-A do CP, segundo a Lei n. 9.983/2000. Em caso de particulares, deveremos analisar as condutas decorrentes da manipulação indevida da base de dados e seus resultados.

8.2.9. Consumação e tentativa

A consumação ocorre com a constatação da invasão, esta comprovada por prova pericial, que avaliará os artefatos e evidências como data e hora de conexão (*login*) e data e hora do fim da conexão (*logout*).

O chamado *footprinting*, ou mesmo o *scan*, diga-se, o envio de pacotes para um dispositivo para avaliar suas "portas abertas", vulnerabilidades, serviços rodando, dentre outras informações, embora possa resultar da obtenção de *flags* ou dados, não se incluem em prova de invasão, constituindo, no máximo, atos preparatórios, não puníveis na legislação criminal brasileira, em que pese coletarem algumas informações, como mencionado.

A invasão não pode se dar por presunção, mas deve ser comprovada com um mínimo de elementos que possam indicar que, efetivamente, em determinada data/hora de um determinado fuso horário (GMT), uma conexão não autorizada foi bem-sucedida, proveniente de determinado IP (Internet Protocol), mediante determinada técnica de intrusão, explorando determinada vulnerabilidade, tendo durado pelo tempo estabelecido e tendo o agente tentado ou realizado determinadas ações.

Importante destacar novamente o entendimento de parte da doutrina, sobre o tema envolvendo tentativa, crime impossível e arrependimento eficaz, que assevera que a leitura de dados tem como resultado a compreensão dos mesmos (sendo considerada "obtenção", mesmo que não tenha havido cópia), mas se estiverem criptografados, haverá a hipótese de crime impossível. Já a escrita dos dados tem como resultado a alteração, porém se o agente altera os dados e na sequência, arrependido, restaura tudo ao estado anterior, estaremos diante do arrependimento eficaz, previsto no art. 15 do Código Penal (VIANNA e MACHADO, 2013, p. 67).

Dispositivos que serão grandes registradores destas atividades (invasões) são os conhecidos *firewalls*, SIEMs (*Security Information and Event Management*), IDS (*Intrusion Detection Systems*), dentre outros, que deverão estar atualizados e configurados para registrar tais informações[70], impedindo ao máximo manipulação humana para evitar "provas criadas" ou contaminações. Mais uma vez verificamos que a segurança da informação é impactada pela Lei n. 12.737/2012, exigindo um padrão adequado de registro das atividades em uma rede ou dispositivo informático.

Entretanto, a Lei n. 12.737/2012 não dispõe sobre qualquer obrigatoriedade das empresas

provedoras de serviços ou de conexão em custodiarem os registros (*logs*) de conexão ou de acesso a aplicações, considerando eventual necessidade de uma investigação para apuração da autoria de crimes eletrônicos. Tal obrigatoriedade é prevista na Lei n. 12.965/2014 (Marco Civil da Internet).

No caso de invasões em andamento, poderá a vítima, para comprovar o fato volátil, valer-se de testemunhas (comumente pessoas do time de resposta a incidentes) e da chamada “ata notarial”, diga-se, documento público lavrado por tabelião de notas e que atesta que determinado fato aconteceu ou está acontecendo (inclusive no ciberespaço), gozando tal declaração de fé pública. A cadeia de custódia, documento que registra o trânsito das evidências ou artefatos informáticos, deverá ser estabelecida tão logo se constate o incidente.

Já a tentativa também se afigura possível de ser praticada e detectada, por exemplo, na hipótese de um *firewall* (porta corta-fogo), IDS, ou mesmo time de resposta a incidentes que detecta um ataque de força bruta (*brutal force*) ou *code injection* objetivando *ownar* (tornar-se proprietário) ou tomar o superusuário de determinada máquina, e que impede o ataque. Todo o proceder deve ser ágil no que tange à coleta de provas, pois a qualquer momento as evidências podem desaparecer.

Nestes casos, a doutrina assevera ser possível também a hipótese da chamada legítima defesa cibernética ou informática, que será vista no item 8.2.11.

Via de regra, neste contexto, o tipo previsto no art. 154-A do Código Penal é um delito onde a perícia forense computacional (informática forense) será indispensável, pois para que a invasão possa ser efetivamente provada, deverá ser determinada a realização de perícia, nos termos do art. 158 do Código de Processo Penal, admitindo-se excepcionalmente a prova testemunhal (art. 167 do Código de Processo Penal).

É somente o perito digital, sob pena de nulidade da ação penal, que poderá atestar se houve invasão, precisar a técnica ou ferramenta utilizada, atestar se foi consumada ou tentada a ação, ponderar se havia efetivo mecanismo de proteção, avaliar se o item invadido é realmente um dispositivo informático e, principalmente, avaliar se o mecanismo de segurança precisou ser violado

pelo agente, dentre outras análises, e, com base nos artefatos e evidências levantadas, atestar se a intenção do agente era criminosa ou não.

Um dos quesitos essenciais que veremos, e que deverá ser formulado ao perito pelo Delegado de Polícia, Ministério Público ou pelo Juiz de Direito, será se no dispositivo havia mecanismo de segurança. Além disso, deverá haver no expediente orientação ao *expert* para descrever a forma da invasão (*modus operandi*). O perito deverá, nos termos do Código de Processo Penal, zelar para que sua análise possa ser repetida ou reproduzível.

8.2.10. Concurso de crimes

Pode haver concurso material do delito do art. 154-A (invasão) com outros crimes, como, por exemplo, quando ocorre, antes da invasão, o roubo (art. 157) ou o furto (art. 155) do dispositivo informático.

O agente, valendo-se de suítes para invasão, pode, com um clique, disparar uma série de ataques que ofendam diversos bens jurídicos. A exemplo, o agente que executa uma única instrução, um comando que permite a invasão e a interrupção do serviço informático, logo havendo a possibilidade do concurso formal. Outro exemplo é o caso em que o agente dispara a invasão em face de diversos *hosts*, obtendo acesso em vários deles.

Mais um exemplo de concurso formal pode ser obtido no caso do agente que invade, mediante uma ação em um servidor IAAS (*Infrastructure as a Service*) de um provedor de *Cloud Computing* (servidores nas nuvens), discos virtuais de diversos clientes. No caso de *Cloud Computing*, o agente, sem saber, com uma ação pôde acessar indevidamente dispositivos diversos, caso em que estaremos diante do concurso formal. Destaca-se que se o agente desconhece esta circunstância, não há que se falar em concurso de crimes.

Existe ainda concurso formal quando o agente, mediante *software* específico e uma ação, invade roteador *wireless*, quebrando chave de segurança, ao mesmo tempo interceptando comunicações dos

que utilizam tal Internet, onde visualizamos o concurso do art. 154-A (agravado pela obtenção de conteúdo de comunicação) com o art. 10 da Lei n. 9.296/96, considerando que o agente realizou interceptação telemática em si[71].

É possível cogitar-se também em crime continuado, quando o agente executa as mesmas rotinas de invasão, nas mesmas condições de tempo e lugar, praticando diversos crimes, caso em que responderá nos termos do art. 71 do Código Penal.

Não poderá haver concurso do delito do art. 154-A com o crime de dano (art. 163), nem com o crime de divulgação de segredo (art. 153) e com a violação de segredo profissional (art. 154), podendo se cogitar em concurso envolvendo delitos de propriedade imaterial, nos termos do art. 195 da Lei n. 9.279/96, bem como envolvendo delitos ofensivos à honra, como difamação, injúria e calúnia.

8.2.11. Legítima defesa informática

Se uma vítima, ao descompilar um *trojan* de que fora vítima, descobre *e-mail* e senha para onde as informações bancárias estavam sendo enviadas, pode querer acessar tal conta para levantar informações sobre um criminoso digital ou apagar seus dados.

Vítimas, pessoas físicas ou jurídicas, podem, em caso da detecção de um ataque em andamento, constituindo uma injusta agressão, buscar interromper o ataque, mas também apurar a autoria por meio de provas que podem ser produzidas em uma espécie de "contra-ataque". E tecnologia existe, considerando que muitas empresas hoje têm conhecimentos e equipe de resposta a incidentes aptas a detectar ataques em tempo de execução.

Uma empresa poderia acessar a conta de um servidor *FTP* (*File Transfer Protocol*) de um criminoso digital e lá apagar segredos ou informações sigilosas furtadas ou copiadas após a invasão, visando impedir a divulgação? Poderia acessar um *e-mail* descoberto na engenharia reversa de um código malicioso e lá obter informações sobre os crimes do atacante?

Tais afirmações estão relacionadas a um conceito difundido na doutrina brasileira, denominado "legítima defesa informática". Segundo o inciso II do art. 23 do Código Penal, não há crime quando o agente pratica o fato em "legítima defesa". Entende-se, pois, em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem.

Logicamente, a defesa deve se valer de proporcionalidade e não pode servir de subterfúgio para ataques digitais ou exercício arbitrário das próprias razões. Tal instituto pode afastar a incidência do art. 154-A do Código Penal, nos termos da Lei n. 12.737/2012, quando comprovado que a invasão, em resposta, deu-se de forma moderada, pela vítima ou equipe de segurança ou resposta a incidentes, que desenvolveu um protocolo de *Ethical Hacking*, para garantir direitos ou prevenir responsabilidades.

Segundo Crespo (2011, p. 114), acerca da moderação da legítima defesa informática, "mas não se podem generalizar condutas. Se alguém lhe enviar um *spam*, você não pode responder com um vírus".

Parte da doutrina aceita a legítima defesa informática também nos casos em que o agente produz uma prova ilícita ou ilegítima (como a produzida mediante invasão de computador ou dispositivo informático), porém, para demonstrar sua inocência em face do Estado diante de uma persecução criminal e do princípio da verdade real.

Tais institutos, embora teorizados, não se manifestam constantemente em casos no Brasil, porém poderão ser ventilados mais constantemente, com a aprovação da Lei n. 12.737/2012.

Deste modo, a resposta ativa a um incidente poderá não ser criminalizada, se enquadrar-se no contexto da legítima defesa, esta que deverá ser comprovada pela perícia, que deverá apurar se foram utilizados os meios eficazes e suficientes para repelir a injusta agressão (ataque). Neste sentido, faz-se indispensável a capacitação em *Ethical Hacking* aos que ingressem de equipes de resposta a incidentes, para que uma vítima não se transforme em criminosa, em questão de poucos

cliques.

8.2.12. Anatomia da invasão

Invasão pressupõe acesso forçado, mas como importar um conceito do mundo físico para o digital?

Ardil ou artifício seriam técnicas de invasão? O *phishing scam* (*e-mail* malicioso, por exemplo, enviado a vítima com código perigoso) baixado e instalado seria invasão? Para certa corrente, a invasão ocorre quando o agente baixa o código malicioso. Auriney Brito (2013, p. 70) assevera que "uma dúvida que já surgiu é já relacionada justamente a esta prática do *phishing*, uma das mais comuns espécies de fraudes informáticas, em que através de engenharia social, o criminoso faz com que a própria vítima entregue informações que ele precisa, ou que ela mesma desabilite sua segurança para que ele possa acessar livremente os dados. Em primeira análise, neste livro conclui-se que o criminoso poderá ser punido pelo art. 154-A do CP, mesmo que a própria vítima tenha liberado o acesso, ela não agiu de forma consciente, foi induzida em erro, considerando-se, portanto, que houve violação indevida da segurança do computador. Porém, se com habilidade o criminoso conseguir que a vítima entregue o conteúdo informático, sem que haja invasão, não há falar em crime por ausência do verbo núcleo do tipo".

Data venia, discordamos da primeira parte das conclusões. Como veremos adiante (*vide* p. 127 e s.), o *phishing scam* pode se dar por técnicas diferenciadas. Em algumas a vítima não tem consciência de que está abrindo as portas de seu ativo informático. Já em outras, tem (quando, por exemplo, fornece as informações de acesso a um *site* ou ao atacante, ainda que enganada ou sob um falso pretexto). Se convencemos alguém, por qualquer meio, a nos levar para dentro de sua casa, não respondemos por violação de domicílio. Já, se enganamos alguém que, sem saber, abre a porta de sua casa no momento em que entramos, perfazem-se os elementos do tipo da invasão.

Do mesmo modo deve ser na informática: o agente que faz com que a vítima espontaneamente forneça suas credenciais de acesso a um dispositivo ou *site* não pode ser punido por invasão (no

máximo, tentativa de estelionato, nos termos do art. 171, o que para muitos também é enquadramento mais que forçoso). Já o agente que envia código malicioso, fazendo com que a vítima, sem consciência, acabe por abrir seus ativos ao executar o código, no mínimo responderá pelo art. 154-A do Código Penal, se outro crime mais grave não decorrer da conduta, como furto mediante fraude em modalidade tentada ou consumada. Cada situação deverá ser analisada em detalhes.

Assim como no crime de violação de domicílio, na Lei n. 12.737/2012, deve ser entendido como sujeito passivo aquele que tem direito de admitir ou excluir alguém do acesso a um dispositivo informático.

A invasão pode se dar a um dispositivo com diversas contas de usuário, como, por exemplo, um computador com contas de todos os membros da família. Quem será vítima? Em nosso entendimento, aquele cuja conta foi usada poderá responsabilizar o agente, ainda que não seja proprietário do dispositivo. Igualmente, o proprietário do computador terá legitimidade ativa.

Pode ocorrer de a pessoa ter consentimento para acessar ou testar um sistema. O consentimento exclui, logicamente, a tipicidade. Por outro lado, a qualquer momento essas permissões podem ser revogadas. Na invasão de domicílio, prevista no art. 150 do Código Penal, existe o delito também pelo "permanecer" na casa, sem autorização. A Lei n. 12.737/2012 silencia a respeito do agente que, tendo permissão para acessar o dispositivo, nele permanece após a revogação ou cancelamento desta permissão.

Devem as autoridades, amparadas pela perícia, apurar exatamente as permissões existentes à data do acesso, e, principalmente, se existiam, se foram revogadas e comunicadas, pois o agente poderá alegar que desconhecia sua ausência de permissão.

8.2.13. Ação penal e competência

Trata-se de crime que se apura mediante ação penal pública condicionada à representação. Diga-se, faz-se necessária a autorização da vítima como condição de procedibilidade para a propositura

da ação penal pelo Ministério Público. Já nos crimes cometidos contra a Administração Pública, direta ou indireta, a ação é incondicionada. Vejamos:

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

O crime de invasão de dispositivo informático, considerando pena inferior a 2 (dois) anos, será processado em face do Juizado Especial Criminal. Por outro lado, considerando a complexidade probatória dos delitos desta natureza, a competência poderá ser deslocada para a justiça comum[72].

8.3. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

8.3.1. Conceito

Um dos principais crimes puros cometidos no mundo cibernético é a indisponibilização de serviços, diga-se, ataques que atentam contra a intermitência de um serviço de tecnologia da informação. A principal técnica utilizada para estes ataques é a chamada DoS (acrônimo em inglês para *Denial of Service*) ou ataque de negação de serviços.

Um ataque de negação de serviço é uma tentativa de tornar recursos de um sistema indisponíveis para quem os utiliza, sendo os alvos mais comuns os servidores *Web*. É preciso esclarecer que não se trata de invasão de sistemas ou dispositivos informáticos, mas de nítida invalidação pela sobrecarga.

Além do DoS, outra derivação deste ataque, muito potente e que vem sendo cada vez mais utilizada em manifestações de ativismo cibernético, é a DDoS (*Distributed Denial of Service*). Nesta modalidade, um computador "Mestre" pode assumir o comando de centenas ou milhares de outras máquinas, os "Zumbis", podendo ordenar que eles ataquem determinado alvo em certa data e hora, o

que torna mais fácil alcançar o objetivo de indisponibilizar os serviços[73].

Alguns vírus conhecidos criados para rotinas de ataques de negação de serviço incluem o Codered, MyDoom, Slammer, sendo códigos que escravizam a vítima, que passa a servir de Zumbi. Dentre os principais ataques de negação de serviço, podemos citar o Ping Flood, no qual o atacante sobrecarrega a vítima com pacotes ICMP Echo Request (pacotes *ping*) e o SynFlood[74], que é um ataque que explora o conceito Three-way-handshake, o famoso “aperto de mão” em três etapas para o estabelecimento de uma conexão TCP (*Transmission Control Protocol*), permitindo a comunicação pela Internet.

Nesta forma de ataque de negação de serviços, o atacante envia uma sequência de requisições SYN para um sistema alvo objetivando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação. Normalmente, quando um cliente inicia uma conexão TCP, este e o servidor trocam uma série de mensagens, sendo que o cliente inicia solicitando uma sincronização (SYN), o servidor responde confirmando a solicitação (SYN-ACK) e, por fim, o cliente responde para que a conexão seja estabelecida (ACK). No ataque SynFlood, que explora a boa-fé do protocolo TCP-IP, o cliente, um criminoso digital, simplesmente não responde a última mensagem (ACK), para que a conexão seja estabelecida e, neste caso, o servidor aguardará um tempo pela conexão que nunca será efetivada. Esta sequência, realizada milhares de vezes, onera os serviços do servidor, que negará serviço.

Nestes casos, o recurso afetado pode reiniciar, desligar, travar ou simplesmente não responder a requisições de clientes legítimos, onde os prejuízos podem ser cavalares, sobretudo se falamos de infraestruturas críticas de saúde, energia, telecomunicações etc.

O art. 266 do Código Penal não era expresso ao tratar da possibilidade de sistemas informáticos serem objeto do ataque envolvendo a interrupção. Tal lacuna é suprimida com a Lei n. 12.737/2012, que complementou o dispositivo, que passa a vigorar com a seguinte redação:

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir

ou dificultar-lhe o restabelecimento:

Pena – detenção, de 1 (um) a 3 (três) anos, e multa.

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Trata-se de crime formal, de forma livre, comissivo ou omissivo. Para alguns doutrinadores, é também crime de perigo abstrato.

8.3.2. Objetividade jurídica

Busca-se com o presente tipo penal proteger a regularidade dos serviços telegráficos, radiotelegráficos, telefônicos e, a partir da Lei n. 12.737/2012, os serviços telemáticos ou de informação de utilidade pública.

Serviços de utilidade pública são aqueles que objetivam facilitar a vida do indivíduo na sociedade, colocando à disposição deste utilidades que lhe proporcionarão mais conforto e bem-estar. Ao contrário dos serviços públicos, que visam manter necessidades gerais e essenciais da sociedade para que elas possam se desenvolver, os serviços de utilidade pública atendem às conveniências de membros da sociedade individualmente considerados.

A telemática pode ser entendida como o conjunto de tecnologias de transmissão de dados que resultam da união de recursos de telecomunicações e da informática, e que permitem o processamento, a compressão, o armazenamento e a comunicação de dados. Serviços telemáticos, por consequência, resultam da associação da informática com as telecomunicações para promover o uso da informação de maneira mais interativa e eficaz.

Deste modo, não só o serviço telemático é protegido, mas, antes dele, o próprio serviço de informação. A telemática potencializa e amplia um serviço de informação.

Destaque-se, também, que se a lei protege serviços de utilidade pública não essenciais, mas que

proporcionam benefícios a determinados cidadãos, entendemos que serviços públicos informáticos também são objeto jurídico da legislação. Nesse contexto, poderíamos inserir alguns aplicativos sociais oferecidos por prefeituras, hospitais, polícias, entre outros.

É preciso que se esclareça que o dispositivo tem por escopo o funcionamento do serviço de comunicação, considerado em seu conjunto geral, no interesse coletivo e não individual. Assim, a interrupção de um serviço específico, para fins de aplicação do dispositivo em comento, dependerá da avaliação se efetivamente agrediu o interesse coletivo ou trouxe perigo comum.

Além disso, tem-se que a pena é majorada em dobro, quando o delito se der por ocasião de calamidade pública.

Segundo Tulio Vianna e Felipe Machado (2013, p. 104),"trata-se de crime contra a incolumidade pública, o que pode ser facilmente constatado até mesmo por sua localização no Título VIII do CPB. Esse crime, portanto, abarca tão somente condutas que atingem um número indeterminado de pessoas e nunca uma vítima ou grupo de vítimas determinado".

Nesta linha de raciocínio é um erro imaginar que a legislação protege especificamente alguém (um particular, por exemplo) da interrupção ou perturbação de um serviço de informação ou informático específico, que lhe pertença.

8.3.3. Classificação criminal

O art. 266 do Código Penal comina pena para aquele que interrompe ou perturba serviço telegráfico, radiotelegráfico ou telefônico, sendo esta de detenção de um a três anos e multa. Com advento da Lei n. 12.737/2012, acrescenta-se o § 1º ao art. 266, dispondo que na mesma pena incorre aquele que interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. Percebe-se que a mera perturbação, em se tratando de serviço telemático ou de informação, não é punível, devendo, para restar caracterizado fato criminoso, haver comprovação da efetiva "interrupção" do serviço telemático.

Deve-se destacar que a lei só protege o serviço telemático ou de informação que seja de utilidade pública, critério difícil de se definir atualmente e que deverá ser apreciado pelo magistrado em cada caso. Deve-se destacar que é conduta criminosa, também, impedir ou dificultar o restabelecimento de um serviço telemático ou de informação.

Destacam-se, aqui, as hipóteses onde a interrupção não foi causada pelo agente, mas este, podendo ou tendo condições para restabelecer o serviço, nada faz, hipótese na qual está caracterizado o delito. O agente administrador de um *site*, que descobre uma *shell* executando em seus servidores, realizada para atentar contra um alvo, que saiu do ar, pode responder se não adotar medidas imediatas para remover o código malicioso.

Trata-se de crime instantâneo, eis que, uma vez interrompido o serviço por um instante, a conduta não pode mais ser cessada pelo agente, eis que já ocorrida. É também delito de fato permanente, exigindo-se o corpo de delito para provar a interrupção, considerando tratar-se de crime que deixa vestígio.

É, via de regra, um crime comissivo, exigindo uma atividade positiva do agente, que realiza ato capaz e idôneo a interromper um serviço telemático ou de informação. Pode ser considerado um delito de conduta mista, à medida que, apesar de poder exigir uma conduta ativa do agente, por vezes, o agente pode praticar o delito por não fazer o que era devido, como, por exemplo, não habilitando as proteções do sistema que se tornou indisponível.

A interrupção de serviço telemático, impedindo ou dificultando seu restabelecimento pode ser considerado crime unissubjetivo, eis que pode ser realizado por uma única pessoa, embora na maioria das vezes seja praticado, no universo da informática, em coautoria ou participação (em determinados casos, inclusive, em uma coautoria em que os agentes sequer se conhecem, cada qual em uma localidade do mundo).

Deve-se considerar também a progressão criminosa, em que o agente será punido pelo delito mais grave em casos que, por exemplo, o agente precisou invadir os servidores antes de "interromper" as

atividades, ou mesmo no caso em que, após a interrupção, ocorre o dano ou mesmo o acesso indevido a dados. Lembrando que os fatos deverão se dar, para a progressão criminosa, sempre no mesmo contexto, o que poderá restar provado da prova técnica. Pode ser, de acordo com o caso concreto, crime exaurido, na medida em que, após praticado o delito do § 1º do art. 266 do Código Penal, pode o agente levar a consequências mais lesivas. O juiz deverá considerar tais circunstâncias na aplicação da pena.

Trata-se de crime de ação múltipla, considerando que o tipo penal traz diversas modalidades de conduta, ou seja, interromper serviço telemático ou de informação, impedir ou dificultar o restabelecimento.

Igualmente é crime plurissubsistente, composto por vários atos que integram a conduta. Quanto ao resultado, é crime material, exigindo para sua consumação o resultado previsto no tipo. Admite a figura da tentativa e é também crime de dano, eis que só se consuma com a efetiva lesão ao bem jurídico protegido. Trata-se de crime comum, podendo ser praticado por qualquer pessoa.

Lembrando que a pessoa jurídica pode figurar como sujeito passivo deste delito. Pode ser, por fim, crime putativo, nos casos em que o agente, por exemplo, vale-se de aplicação que executaria negação de serviços em um sistema informático, porém é comprovado por perícia que tal aplicação não poderia ou não tinha condições de ser utilizada para causar a interrupção.

8.3.4. Sujeito ativo

Qualquer pessoa pode figurar como sujeito ativo dos crimes, incluindo pessoa que realiza os serviços, empregados, prepostos etc.

8.3.5. Sujeito passivo

O sujeito passivo do crime é o Estado. Para muitos autores, sujeito passivo deve ser, necessariamente, um número indeterminado de pessoas (coletividade).

8.3.6. Tipo objetivo

As condutas reprováveis ou núcleos do crime são: a) interromper (cessar, parar); b) perturbar (atrapalhar, modificar, desordenar) a realização de serviços telegráficos, radiotelegráficos e telefônicos; c) impedir (não permitir, inviabilizar); ou d) dificultar (onerar, prejudicar, tornar dificultoso) o restabelecimento dos mesmos.

Importa dizer que, com o advento do § 1º acrescentado ao art. 266 do Código Penal pela Lei n. 12.737/2012, passa a ser objeto material também o serviço telemático ou de informação de utilidade pública. Pune o legislador apenas a interrupção do serviço e aquele que impede ou dificulta o restabelecimento dos serviços, não punindo aquele que “perturba” tais serviços telemáticos, ao contrário do que prevê para os serviços telegráficos, radiotelegráficos e telefônicos, onde, de acordo com o *caput* do art. 266 do Código Penal, também pune-se a mera “perturbação”.

Diga-se, quando o objeto material for o serviço telemático, teve aparente prudência o legislador brasileiro, exigindo, para punição do suposto criminoso digital, que se concretize a interrupção, não bastando a mera perturbação. Tecnicamente, tal medida se mostra coerente, pois do contrário técnicas de farejamento de redes, *footprinting* e rastreamento do *host* ou simples comandos de *ping* poderiam ser considerados criminosos[75].

Um programa como Nmap, um *software* livre criado que realiza o chamado *portscan*, utilizado para avaliar a segurança dos computadores, descobrir serviços ou servidores em uma rede de computadores, gera registros (*logs*) nos sistemas avaliados, o que poderia motivar uma empresa a registrar uma queixa-crime por suposta perturbação de serviço telemático. Assim, o uso de qualquer programa que gerasse ruído poderia ensejar um inquérito policial, o que seria absurdo.

Deve-se ponderar que o art. 266 do Código Penal pune a interrupção ou perturbação do serviço telegráfico, telefônico ou telemático, ou seja, pune quem atenta contra todo o sistema ou parte dele. Logo, aquele que inutiliza equipamento utilizado pelo serviço pode apenas responder pelo crime de dano, previsto no art. 163 do Código Penal.

Igualmente, aquele que interrompe ou perturba o funcionamento de apenas um aparelho (que pode ser telemático), ou mesmo dificulta ou impede certa comunicação entre pessoas determinadas, pode responder pelo crime previsto no art. 151, § 1º, III, do Código Penal.

8.3.7. Tipo subjetivo

Não existe a necessidade de qualquer elemento subjetivo especial do tipo. O elemento subjetivo é o dolo, ou seja, a vontade consciente de interromper ou perturbar os serviços do tipo penal, ou mesmo impedir ou dificultar o seu restabelecimento.

Logo, se comprovado que o computador do agente estava infectado por *trojan*, *botnet* ou qualquer código malicioso que executava instruções ao computador para interromper determinado serviço de outrem, sem que o titular soubesse, não há que se falar no crime em tela.

Deve-se destacar que o agente que interrompe o serviço pode não ser o mesmo que impede ou dificulta seu restabelecimento. Tais situações dependerão de perícia técnica especializada para avaliar a materialidade e a parcela de participação de potenciais envolvidos em incidentes dessa natureza.

Como exemplo, podemos citar o agente "A" que, acessando sistema da vítima, exclui arquivos de um serviço, que é interrompido. A vítima comunica ao agente "B", administrador da rede, único com a senha de acesso *root*, para que acesse o sistema ou adicione um usuário para que as correções sejam realizadas e o sistema restabelecido, porém este dificulta o restabelecimento, exigindo determinada quantia para o fornecimento da credencial ou correção do problema.

Tal assertiva também vale para titulares de provedores de serviços, que, diante de sistemas comprometidos de clientes, recusam-se a cooperar para o pronto restabelecimento dos serviços.

8.3.8. Consumação ou tentativa

A consumação do crime se dá com a efetiva interrupção ou perturbação (no caso do *caput* do art.

266), devidamente comprovada por laudo pericial, ou quando o sujeito ativo impede ou dificulta o restabelecimento do serviço. Mais uma vez, chamamos a atenção para a volatilidade e dificuldade da prova em casos de perturbação ou mesmo para se comprovar o impedimento para restabelecimento dos serviços.

Em nosso sentir, todos os meios legais e moralmente legítimos são aptos para a produção desta prova, mas dependerão de uma adaptação técnica dos serviços de TI para que possam capturar provas que podem se esvair no espaço em questão de segundos, como, por exemplo, a latência ou lentidão em uma rede provocada por um agente específico (perturbação).

Apesar de se tratar de crime de perigo abstrato, segundo alguns doutrinadores, em tese, seria admissível cogitar de situações em que a própria tentativa de interrupção não possa ser considerada uma perturbação, questões que dependerão de análise técnica pericial. No caso de serviço informático em que se pune apenas a interrupção, a perturbação poderá, dependendo do caso, ser considerada tentativa.

8.3.9. Ação penal

Pública incondicionada. Competência do juízo comum e não do Juizado Especial Criminal.

8.4. Falsificação de documento particular

8.4.1. Conceito

Antes mesmo da "Lei Carolina Dieckmann", tinha-se como práticas jurisprudenciais e certo consenso na doutrina relativa ao Direito da Tecnologia da Informação o dever do usuário na formação, custódia e renovação de suas senhas, pois estas são, na sua gênese, o que identifica um usuário no mundo cibernético, consequentemente, uma pessoa física ou jurídica.

De maneira que, sendo as senhas as assinaturas eletrônicas de uma pessoa na rede (ou, pelo menos,

critérios de identificação – autenticidade), quem as decifra, em verdade, estaria falsificando uma assinatura. Hoje, já dispomos de outros métodos de autenticação que, por exemplo, consideram outros fatores, não só o que um indivíduo sabe, mas o que ele tem ou mesmo o que ele é (fatores biométricos).

Quando falamos sobre algo que o usuário tem, podemos nos referir ao velho cartão de crédito, diga-se, um “plástico” indispensável para que uma transação financeira seja aceita (temos também *tokens*, OTPs etc.). Logo, mais uma vez, quem consegue “clonar” este plástico, novamente está falsificando a assinatura de alguém, forjando sua identidade.

Até mesmo dispositivos celulares podem ser utilizados para a realização de transações financeiras, no conceito denominado *m-payment*.

Aparentemente, o primeiro caso envolvendo a prisão de um *hacker* no Brasil está relacionado à utilização indevida de dados de cartão de crédito, no ano de 2002, em condenação proferida pela Justiça Federal, pela denúncia de clonagem de *sites* de instituições bancárias do Brasil e do exterior e pela aplicação de golpes em correntistas por intermédio da Internet[76].

A falsificação de documento particular ou alteração de documento particular verdadeiro já era considerada crime pelo art. 298 do Código Penal, prevendo pena de reclusão de um a cinco anos e multa. O que a Lei n. 12.737/2012 fez foi inserir um parágrafo onde equipara ao documento particular o cartão de crédito ou débito.

Assim temos o novo tipo penal, já alterado:

Art. 298. Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro.

Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Parágrafo único. Para fins do disposto no caput*, equipara-se a documento particular o cartão de crédito ou débito.*

8.4.2. Objetividade jurídica

O bem jurídico protegido é a fé pública, no que tange à autenticidade e integridade dos documentos particulares. Tem-se que a falsificação grosseira exclui o crime, considerando que não há perigo à fé pública.

Documentos registram há séculos fatos e manifestações de vontade da humanidade. O documento, para ser considerado como tal, deve ter relevância jurídica em seu conteúdo e não deve ser anônimo.

Para a caracterização do crime faz-se indispensável o exame de corpo de delito, sendo também imprescindível a apresentação do documento falsificado. A questão torna-se complexa quando a falsidade for informática, onde o plástico (cartão de crédito ou débito) permanece na posse da vítima, mas o atacante obteve acesso aos códigos e à numeração dos mesmos, fazendo-se passar pela vítima em *sites* e realizando compras em seu nome.

Como realizar o corpo de delito? A Perícia Forense Computacional, especializada em informática, terá papel relevante para coletar as informações e registros que representem a "falsificação", bem como em detalhar didaticamente tal representação a um Juiz de Direito.

Com o surgimento das tecnologias, documentos passaram a ser representados em outros suportes que não a cártula, porém constitui um desafio jurídico ainda pouco enfrentado. Poderíamos interpretar extensivamente o art. 298 para compreender as falsidades virtuais e o uso indevido dos dados de um cartão de crédito? Em nosso entendimento, não.

8.4.3. Classificação criminal

A Lei n. 12.737 acrescentou um parágrafo único ao art. 298 do Código Penal, que trata do crime de "falsificação de documento particular", prevendo uma pena de reclusão de um a cinco anos e multa, se o documento é público, e reclusão de um a três anos, se o documento é particular.

O parágrafo único inserido prevê que se equipara a documento particular o cartão de débito ou crédito. O escopo do legislador foi fazer frente às fraudes bancárias envolvendo clonagem de

cartões. Porém, o artigo não se aplica às fraudes financeiras praticadas pela Internet.

Trata-se de crime instantâneo, considerando que, uma vez consumado, está encerrado. É também crime de fato permanente, sendo indispensável o corpo de delito. Igualmente, é crime comissivo, exigindo-se conduta positiva do agente, diga-se, um fazer, consistente em falsificar um cartão de crédito ou débito.

O agente que consegue romper criptografia de um cartão legitimando-o ou, de certo modo, utilizando-o, pode responder pela segunda parte do tipo, diga-se, a alteração de documento particular verdadeiro. É crime unissubjetivo, podendo ser praticado por apenas uma pessoa, nada impedindo a coautoria, podendo ser considerado, também, crime simples.

Por outro lado, a recarga clandestina de créditos em um cartão de metrô, por exemplo, em tese, não poderia ser equiparada a cartão de crédito ou débito – para fins de aplicação do parágrafo único do art. 298 do CP – no hipotético caso de um agente que consegue recarregá-lo mediante manipulação e quebra da criptografia. É forçoso comparar um cartão de bilhete a um documento particular, podendo o agente, neste caso, responder por invasão de dispositivo informático na medida em que rompeu o mecanismo de segurança do cartão, permitindo a recarga de créditos sem nada pagar.

Pode ser crime exaurido se, da conduta realizada, o agente, na sequência, leva a outras consequências lesivas. É crime de ação múltipla, considerando os verbos previstos no tipo: é punido não só quem falsifica um cartão de crédito ou débito, como quem altera no todo ou em parte cartões verdadeiros. Também se enquadra o delito em estudo no conceito de crime plurissubsistente, considerando que a conduta é preenchida por meio de vários atos, admitindo-se a tentativa.

É crime comum, podendo ser praticado por qualquer pessoa e também crime formal, diga-se, não havendo necessidade do agente ter tido êxito com a falsificação. É também crime de perigo abstrato, segundo alguns doutrinadores. Para nós, essa classificação (perigo abstrato) não subsiste diante da Constituição Federal de 1988 (considerando o princípio do estado de inocência e princípio da culpabilidade).

8.4.4. Sujeito ativo

Pode ser qualquer pessoa.

8.4.5. Sujeito passivo

São o Estado e, secundariamente, a pessoa lesada.

8.4.6. Tipo objetivo

Tem-se por objeto material aqui o documento particular, que pode ser considerado todo o escrito, atribuível a um autor, com fatos ou manifestações de vontade e com relevância jurídica. Entende-se por documento particular aquele que é elaborado sem intervenção de funcionário ou de pessoa que tenha fé pública. Contrato, cheque, declaração, cartão de débito ou crédito, dentre outros.

8.4.7. Tipo subjetivo

Pune-se a modalidade dolosa consistente na vontade consciente em falsificar, no todo ou em parte, documento particular, ou alterar documento particular verdadeiro.

Assim, responde pelo crime tanto o agente que cria cartão de crédito ou débito “clonado” ou falsificado como aquele que adultera cartão alheio para obtenção de determinada vantagem.

8.4.8. Elemento normativo

É crime formal, onde a mera falsificação (elemento normativo) já preenche os elementos do tipo penal, não havendo que se investigar se o agente efetivamente causou prejuízo. Assim com um cheque adulterado, desde que a falsificação não seja grosseira, já se pressupõe a prática do delito, diga-se, uma ordem de pagamento falsa.

Importante esclarecer que a falsidade aqui é material, diga-se, quanto à forma do documento, a

adulteração que cria um documento novo, bem diferente da falsidade ideológica, em que o documento é verdadeiro, mas a declaração é falsa, sendo que a declaração não corresponde à verdade.

8.4.9. A questão do **phishing scam** *(pescaria de senhas)*

O *phishing scam* é uma das principais técnicas utilizadas para golpes e fraudes virtuais no Brasil. Somente no segundo trimestre de 2012, a alta no golpe cresceu 89%[77]. O país é o quarto do mundo com vítimas de crimes virtuais[78].

Ao contrário do que alguns imaginam, tal delito não veio para criminalizar o *phishing scam* (ou pescaria de senhas), mas tão somente punir a clonagem física de plásticos (cartões).

Em um enquadramento questionável, a clonagem de cartão e realização de saques na conta do titular era considerada furto mediante fraude para o Superior Tribunal de Justiça[79].

Já se da clonagem decorresse compras em lojas e estabelecimentos, a jurisprudência do mesmo Tribunal entendia ser o caso, também, da caracterização do estelionato[80].

Importa dizer que em ambas as hipóteses, acima ventiladas, haverá sempre a absorção do delito do art. 298 pelo delito mais grave/delito-fim. Neste sentido, a Súmula 17 do STJ dispõe que *quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido.*

8.4.10. Consumação e tentativa

Consuma-se o crime com a falsificação ou alteração do documento, pouco importando se do ato decorreu o uso ou alguma percepção financeira ilícita.

8.4.11. Ação penal

Pública incondicionada.

8.4.12. Da falha ao se equiparar ao documento particular o cartão de crédito ou débito

A Lei n. 12.737/2012 equiparou a documento particular o cartão de débito ou crédito. Sabe-se que hoje tecnologias hodiernas, plásticos, representam informações que são usadas para autenticar uma pessoa na compra de produtos e serviços.

Só que a tecnologia muda, torna-se obsoleta. E quando o cartão se extinguir? O que faremos com a lei? Em verdade, o legislador, na ânsia de responder a um caso célebre, deixou a desejar na reflexão de tal dispositivo. Poderia equiparar os documentos eletrônicos aos documentos particulares para fins de incidência do tipo penal. Basta lembrar que hoje temos documentos em CDs, *pendrives*, *memory sticks*, *chips*, dentre outros, que podem ser falsificados. O certificado digital, por exemplo, que identifica inequivocamente uma parte em uma transação eletrônica, embora tecnicamente difícil, pode ser falsificado.

E nestes casos citados, qual a proteção existente no ordenamento jurídico brasileiro? Simples, não há que se falar em aplicação da Lei n. 12.737/2012, pois esta foi precisa e excessivamente específica ao indicar as tecnologias que se equiparam a documentos particulares. Logo, uma lei que já nasce com lacunas e com prazo de validade atrelado à evolução tecnológica.

O crime para quem falsifica um certificado digital, por exemplo, é uma lacuna legislativa, que ainda ficará a cargo do integrador da norma, limitado aos princípios já cediços.

9.

A INVASÃO DE DISPOSITIVOS INFORMÁTICOS E ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

É sabido que dados e informações constituem recursos cada vez mais importantes para as corporações. A informação, dos ativos valiosos, hoje é o mais importante. Deste modo, sabe-se que "ativo de informação" é qualquer dado ou informação que agregue valor ao negócio.

Segurança da informação é o processo de proteção de informações das ameaças à sua integridade, disponibilidade e confidencialidade. É papel da segurança da informação preservar os ativos informacionais, assegurando:

• *Confidencialidade*: que o acesso à informação esteja restrito a quem dela deva ter acesso.

• *Integridade*: que a informação esteja íntegra, autêntica e consistente.

• *Disponibilidade*: que a informação esteja disponível a quem dela deva ter acesso.

• *Uso legítimo*: que a informação seja usada por pessoas autorizadas.

Soluções de segurança da informação baseadas em tecnologia relacionam-se com o uso de recursos, *softwares*, métodos e práticas para proteger a informação em todo o seu ciclo de vida. Como bem esclarece Adriana Beal (2005, p. 10), "a fim de manter os ativos de informação protegidos contra perda, furto e alteração, divulgação e destruição indevidas, além de outros problemas que podem afetá-los, as organizações precisam adotar controles de segurança – medidas de proteção que abrangem uma grande diversidade de iniciativas, indo dos cuidados com os processos de comunicação à segurança de pessoas, mídias e componentes de TI".

A proteção aos ativos informacionais pode ser preventiva, como, por exemplo, com a adoção de medidas técnicas para impedir um incidente informático. Por outro lado, não se pode garantir que um

sistema é 100% seguro, momento em que nos valemos das proteções reativas ou recuperadoras, que visam à reação a determinado incidente ou mesmo à reparação dos danos causados. A lei criminal vem neste sentido. Mais que isso, a Lei de Crimes Informáticos pode ser caracterizada, na segurança da informação, como uma proteção desencorajadora, eis que o agente criminoso agora sabe que, se for identificado, será responsabilizado na seara criminal.

Aspectos da segurança da informação são impactados com a edição da Lei n. 12.737/2012. Inúmeras atividades desenvolvidas por pesquisadores e empresas necessitam ser refletidas à luz da nova Lei de Crimes Informáticos. Inúmeros controles, planejamentos e políticas precisam ser revisados.

A comunidade de segurança da informação, com olhar técnico, também anseia por respostas em relação às interpretações possíveis do art. 154-A do Código Penal. Refletir sobre as principais vulnerabilidades de sistemas *web* e o possível enquadramento criminal de quem as explora é papel do operador do Direito Penal Informático e o que se ousa realizar no presente trabalho.

O desafio é grande, pois a cada dia novas técnicas, vulnerabilidades e questões poderão surgir e demandar novos estudos e revisões por parte do profissional do Direito da Informática. Condensamos, neste capítulo, os principais e mais polêmicos aspectos envolvendo a segurança da informação e o crime de invasão de dispositivo informático.

Apresentamos, assim, as principais questões relativas ao delito previsto no art. 154-A do Código Penal, trazido pela Lei n. 12.737/2012, em relação a aspectos da segurança da informação e criminalidade informática, no escopo de contribuir para a interpretação e esclarecimento da norma por parte de seus aplicadores.

9.1. Princípio da insignificância na invasão de dispositivo informático

Não se pode desconsiderar que a doutrina admite a teoria do Direito Penal Mínimo e, sobretudo, o princípio da insignificância em determinados delitos informáticos, em que somente bens jurídicos de

maior relevância deveriam ser protegidos pelo Direito Penal.

Ligado aos chamados “crimes de bagatela” (“ou delitos de lesão mínima”), o princípio da insignificância recomenda que o Direito Penal, pela adequação típica, somente intervenha nos casos de lesão jurídica de certa gravidade, reconhecendo a atipicidade do fato nas hipóteses de perturbações jurídicas mais leves (pequeníssima relevância).

Esse princípio tem sido adotado pela nossa jurisprudência nos casos de furto de objeto material insignificante (subtração de um pano de chão, sapatos usados de pouco valor, uma passagem de ônibus etc.); lesão insignificante ao Fisco; maus-tratos de importância mínima; descaminho e dano de pequena monta; lesão corporal de extrema singeleza etc.[81]. Pensamos que o princípio também se aplica a alguns delitos informáticos, cabendo ao juiz apreciar a questão da ínfima violação jurídica.

Tudo pode ser considerado dado eletrônico, mas será que todo dado eletrônico é relevante a ponto de incidir uma penalização daquele que o obtém ou tem a intenção de obtê-lo? O cidadão que acessa indevidamente *firmware* de um *modem* ADSL (Banda Larga) com o fim de lá alterar informações realizando uma “clonagem de mac”, para permitir que sua rede seja compartilhada, deve ser punido com o mesmo rigor daquele que acessa um sistema bancário e indevidamente com o fim de copiar dados que permitem o saque indevido das contas dos correntistas?

O agente que invade base de dados sem dado algum, ou dispositivos informáticos contendo apenas arquivos de sistemas, com o escopo de obter tais “dados”, deveria ser punido da mesma forma do agente que invade cadastro de cartões de crédito de clientes de uma rede de departamentos?

Poder-se-ia considerar a necessária intervenção mínima do Estado, onde a autonomia e liberdade do indivíduo só poderiam ser tolhidas se realmente necessário. Embora a lei não faça distinção entre os tipos e relevância de “dados” que o agente pretende obter, tal sensibilidade caberá ao operador do Direito diante do caso concreto. Teremos que assistir uma construção jurisprudencial a respeito, sobretudo diante da corrente que não admite pensar em “princípio da insignificância” para delitos formais.

Há, em outro cenário, de se cogitar em princípio da insignificância nos casos do § 2º do art. 154-A do Código Penal, que prevê uma causa de aumento quando da invasão ocorre prejuízo econômico. Se o prejuízo for insignificante, não haverá que se cogitar da aplicação da causa de aumento. Mas o crime simples subsiste.

9.2. Eficácia dos mecanismos de segurança e a abrangência do termo "dispositivos informáticos"

Questão em debate na doutrina diz respeito à abrangência dos termos mecanismos de segurança e dispositivos informáticos. Uma rede social poderia ser considerada um "dispositivo informático"? Qualquer proteção poderia ser considerada "mecanismo de segurança"? Nos Estados Unidos, propostas para alteração da CAFA (*Computer and Abuse Fraud Act)* já denotam que os mecanismos de segurança devem ser "efetivos", sobretudo após a morte do ativista Aaron Schwartz.

Neste sentido, manifestou-se Stewart Baker (2013, p. 1), no *website* Opposing Views em 28 de janeiro de 2013[82], acerca da proposta da Electronic Frontier Foundation (EFF) para o CAFA americano, que "I've just looked at the new proposal for revising the Computer Fraudand Abuse Act (CFAA) offered by Orin Kerr, Jennifer Granick, and the EFF. Essentially, they would set a higher threshold for deciding when a hacker has accessed a computer 'without authorization', by requiring, that the defendant circumvent a technological barrier that 'effectively controls' access".

Logo, somente a perícia poderia afirmar se o artefato existente em um dispositivo informático poderia ser considerado "mecanismo de segurança".

Sobre a nebulosidade legislativa brasileira, ressalta Renato Opice Blum (2013, p. 1) que "primeiro ponto para reflexão: a lei restringe a tipicidade da invasão aos casos em que há a violação indevida de mecanismos de segurança. Assim, os dispositivos informáticos não dotados de ferramenta de proteção estariam excluídos da aplicação legal. Ademais, as expressões mecanismo de segurança e dispositivo informático (só *hardwares*? E os *softwares*?) não foram definidas na lei,

restando dúvidas sobre o completo enquadramento de certos casos”[83].

Poderia um dispositivo informático ser afeto à categoria de *software*? Alguém que invade um sistema informatizado estaria incidindo no tipo do art. 154-A do Código Penal? Se positivo, o acesso indevido a *blogs*, *sites*, perfis em redes sociais, dentre outros, estaria coberto pelo disposto no precitado tipo penal? Para Cavalcante (2013, p. 2), dispositivo informático seria um *hardware*: “Em informática, dispositivo é o equipamento físico (*hardware*) que pode ser utilizado para rodar programas (*softwares*) ou ainda para ser conectado a outros equipamentos, fornecendo uma funcionalidade. Exemplos: computador, *tablet*, *smartphone*, memória externa (HD externo), entre outros”.

Deve-se destacar que o mecanismo de segurança identificado por perícia deve estar protegendo o dispositivo daquela invasão específica. De nada adianta o perito constatar a presença de um antivírus, se por padrão a máquina estava com convite de assistência ou acesso remoto habilitado, que foram explorados. O dispositivo de segurança existente deve ter sido violado, no caso concreto. Alguns pesquisadores vão além, embora discordemos deste detalhamento, e chegam a afirmar que, por exemplo, a vítima pode ter um IPS (*Intrusion Prevention System*) protegendo o dispositivo, mas se não tiver regras de *SQL injection* habilitadas, e um ataque desta natureza acontecer, o dispositivo estaria, em verdade, desprotegido pelo IPS ou WAF (*Web Application Firewall*).

Porém, vale o raciocínio. De nada adianta um dispositivo informático com *firewall* se o agente subtrai disco rígido e acessa diretamente (acesso local) o conteúdo – para este tipo de investida, o mecanismo de segurança ideal seria a criptografia. Neste caso, se comprovado que a intenção do agente não era o furto do disco rígido para perceber o seu valor, mas sim acessar as informações, o crime de furto (art. 155) será absorvido pelo delito de invasão de dispositivo informático (art. 154-A do Código Penal).

9.3. A polêmica envolvendo a “ausência de autorização tácita” para acesso ao

dispositivo

Como verificado, para que o agente seja responsabilizado pelo delito de invasão de dispositivo informático, basta que o acesso se dê a um dispositivo contendo mecanismo de segurança, e que este acesso se dê sem autorização expressa ou tácita do titular do dispositivo.

Ao contrário do que pode significar, a ausência de proibição expressa para acesso a um dispositivo não significa autorização tácita para invasão do mesmo. A ausência de proibição expressa significa proibição tácita. Por outro lado, a autorização tácita pode ocorrer quando o titular do dispositivo, embora não manifeste expressamente a concordância com o acesso indevido, não se manifesta diante de um comunicado de um agente. Pode-se dar, ainda, quando o titular do ativo participa de atos negociais que, por sua natureza, pressupõem a possibilidade de acesso ao dispositivo informático.

Como exemplo, citamos o banco que contrata empresa para realização de um *pentest* ou teste de intrusão em seus servidores. O agente titular de uma assistência técnica informática não precisa de uma “autorização expressa” para poder acessar computador enviado pelo cliente para conserto. Isto porque decorre do próprio contrato de assistência técnica a necessidade do acesso ao dispositivo, hipótese em que estamos diante da presença da autorização tácita, perceptível ao homem mediano, e que afasta a incidência do tipo criminal.

Um exemplo controverso seria a vítima que é notificada, por *e-mail* ou outro meio, sobre a existência de falhas em seu dispositivo que permitem o acesso indevido, nada realizando para corrigir tais falhas. Estaria caracterizada autorização tácita? A nosso ver não, pois a ausência de correção pode se dar por incapacidade ou fatores externos e não pela vontade da vítima.

9.4. A invasão de dispositivos informáticos e a pescaria de senhas (*phishing scam*)

Para uma primeira corrente, no contexto da invasão (termo do tipo previsto no art. 154-A do

Código Penal), não estariam inseridos os acessos que foram exitosos graças à própria ação e colaboração do agente lesado, casos de engenharia social, e, principalmente, o *phishing scam* envolvendo engenharia social ou *phishing scam* com código malicioso (técnica utilizada para fazer com que o agente habilite o acesso a seu computador, liberando as portas), considerando que a vítima é que habilita seu computador, acessando conteúdo ou programa malicioso que recebeu, para que o atacante acesse indevidamente.

Essa é a opinião de uma corrente sobre o tema, que descaracteriza completamente a incidência do art. 154-A do Código Penal no *phishing scam*.

Segundo tal linha, o agente que consegue enganar a vítima para permitir acesso a seu computador não pode responder pelo delito de invasão de dispositivo informático, ainda que a ação tenha sido remota e o agente não esteja no mesmo local físico da vítima. Ainda, para o enquadramento da conduta, o Código Penal já traria a resposta, não existindo necessidade de uma lei específica envolvendo delitos informáticos. Assim, diante do *phishing*, poderia-se cogitar do delito previsto no § 4º do art. 155 (se a fraude foi empregada para distrair a atenção da vítima), ou mesmo da hipótese de incidência do art. 171, estelionato (se a fraude é empregada para fazer com que o agente entregue dados ou informações). Ambos podendo ser praticados na modalidade tentada.

No raciocínio proposto por essa corrente, podemos concluir que o agente que induzisse a vítima a lhe passar as senhas de acesso ao seu dispositivo não cometeria crime algum, pois não existe no Brasil crime de "violação de privacidade", muito menos tentado. Já se as senhas forem bancárias, poderíamos cogitar do estelionato, na modalidade tentada.

Para outra corrente, qualquer modalidade de *phishing scam* enquadra-se no art. 154-A, considerando que a fraude poderia ser considerada "instrumento da invasão", com a ressalva da possibilidade de um crime posterior, como previsto no § 4º do art. 155.

A questão não é tão simples assim. Excelente exercício de raciocínio é proposto por Cavalcante (2013, p. 3), a respeito das possibilidades decorrentes da invasão de dispositivo informático: "O

agente tenta invadir o computador da vítima com o objetivo de instalar o *malware* e obter a senha para realizar o furto, mas não consegue: responderá por tentativa de invasão (art. 154-A) e não por tentativa de furto qualificado (art. 155, § 4º, II); o agente invade o computador da vítima com o objetivo de instalar o *malware* e obter a senha para realizar o furto, porém não inicia os atos executórios da subtração: responderá por invasão consumada (art. 154-A) e não por tentativa de furto qualificado (art. 155, § 4º, II); o agente invade o computador da vítima com o objetivo de instalar o *malware* e obter a senha para realizar o furto, inicia o procedimento para subtração dos valores, mas não consegue por circunstâncias alheias à sua vontade: responderá por tentativa de furto qualificado (art. 155, § 4º, II); o agente invade o computador da vítima com o objetivo de instalar o *malware* e obter a senha para realizar o furto, conseguindo efetuar a subtração dos valores: responderá por furto qualificado consumado (art. 155, § 4º, II)".

Nesse sentido, observe-se recente julgado do Tribunal Regional Federal da 4ª Região, publicado em 17-9-2015, que, enfrentando essa questão, assim decidiu:

PENAL E PROCESSO PENAL. HABEAS CORPUS. *CONDENAÇÃO POR FURTO QUALIFICADO MEDIANTE FRAUDE. ART. 155, § 4º, II, DO CÓDIGO PENAL. SUBTRAÇÃO DE VALORES DE CONTA BANCÁRIA. TRANSFERÊNCIAS VIA INTERNET. DESCLASSIFICAÇÃO DA CONDUTA. ART. 154-A DO CÓDIGO PENAL. INVASÃO DE COMPUTADOR. INCABIMENTO. 1. A subtração de valores de conta bancária, mediante transferência fraudulenta via internet, sem o consentimento do correntista, configura o crime de furto qualificado, previsto no art. 155 , § 4º, II, do Código Penal, sendo improcedente a pretensão de desclassificar o fato para o delito de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, incluído pela Lei n. 12.737, de 2012. 2. Hipótese que não configura aplicação de lei posterior mais benéfica, pois a nova lei, invocada na impetração, já estava em vigor na data da prolação da sentença condenatória e do acórdão que a manteve (*Habeas Corpus 50213979020144040000 5021397-90.2014.404.0000 – TRF-4).

No que tange ao agente que consegue a senha da vítima por meio de engenharia social, importante destacar também que parte da doutrina não considera a conduta criminosa. Tulio Vianna e Felipe Machado (2013, p. 63) entendem que "em tal hipótese, a execução da invasão só se iniciará quando o usuário tentar se autenticar no sistema usando a senha obtida pela 'engenharia social'. As fases anteriores são meramente preparatórias, pois o *cracker* pode obter as senhas por meio de 'engenharia social' sem, no entanto, jamais tentar acessar o sistema da vítima, o que não constitui sequer uma ameaça real aos dados protegidos. Em uma analogia com o crime de homicídio, podemos dizer que o agente comprou a arma, mas ainda não mirou, muito menos apertou o gatilho".

Já se com a senha obtida mediante enganação o agente acessa o sistema, não se pode deixar de consignar entendimentos no sentido de que se o agente conseguiu a senha via engenharia social e acessou o sistema, o fez indevidamente (acesso indevido), mas em tese não praticou delito de invasão, considerando que acessou por meio não forçoso, que não rompeu obstáculo algum, não violou mecanismo de segurança, tendo acessado o sistema por meios ordinários (convencionais), diga-se, simplesmente, digitando um nome de usuário e senha válidos. Importante mencionar: não basta o acesso indevido para a aplicação da Lei n. 12.737/2012, mas é imperioso que ocorra a "invasão".

Mas outra dúvida surgiria neste cenário mencionado. Qual seria o mecanismo de segurança aplicável e suficiente a conter a "engenharia social", para que a obtenção de dados, mediante tal técnica, pudesse incidir no disposto do art. 154-A do Código Penal? Para alguns pesquisadores, a comprovação de "treinamento da equipe" em segurança da informação e em engenharia social, poderia ser considerada um "mecanismo de segurança". Tal linha se assemelha muito àquela daqueles que entendem que a obtenção de senha mediante engenharia social e acesso ao dispositivo é crime previsto no art. 154-A, sem a necessidade de perquirir maiores detalhes.

Assim, em síntese, temos as seguintes correntes identificadas:

Corrente A: o *phishing scam*, a despeito de sua forma de aplicação, enquadra-se no art. 154-A do Código Penal (invasão de dispositivo informático), pois a fraude é o meio da invasão;

Corrente B: o *phishing scam* não se pode enquadrar no art. 154-A do Código Penal (invasão de dispositivo informático), considerando que se trata de fraude, golpe, e não invasão de dispositivo informático, mediante violação de mecanismo de segurança.

Nosso entendimento sobre o tema diverge da primeira e da segunda corrente que expusemos. Isso porque não entendemos que o *phishing scam* não possa, em nenhuma hipótese, ser enquadrado no delito previsto no art. 154-A do Código Penal; explicamos detalhadamente, inclusive fornecendo exemplos oriundos do tipo envolvendo violação de domicílio, por meio de nosso quadro:

a) *Phishing scam* (engenharia social) – A vítima fornece os dados (senhas, *logins*) espontaneamente ao agente que acessa o dispositivo. Não há de se cogitar da aplicação do art. 154-A (invasão de dispositivo informático), podendo-se falar em estelionato na modalidade tentada ou consumada, a depender da informação obtida. O agente que ilude uma jovem a fornecer sua senha de acesso remoto a seu dispositivo, momento em que copia algumas fotos que estavam protegidas contra acesso público, não pratica crime algum. Já o agente que pratica o mesmo ato, mas obtém dados de acesso ao *netbanking*, se acessá-lo poderá responder por estelionato tentado. *Exemplo análogo:* agente que se passando por "fiscal da dengue" convence a vítima a voluntariamente abrir o portão e ingressa na casa. Não há crime de violação de domicílio. Houve o consentimento, ainda que mediante enganação.
b) Invasão – O agente, por meio de técnicas, programas, conceitos, destreza e habilidade, invade dispositivo informático, violando mecanismo de segurança, com o fim previsto em lei. Aplica-se o delito previsto no art. 154-A (invasão de dispositivo informático). *Exemplo análogo:* agente que pula o muro da residência, invadindo domicílio, sem conhecimento ou consentimento da vítima. c) *Phishing scam* (*malware* ou código malicioso) – A vítima recebe e executa um arquivo ou acessa um código induzido pelo atacante e, sem saber, destrava os mecanismos de segurança do seu dispositivo ou fornece ao agente automaticamente os códigos para acesso ao mesmo dispositivo. Aplica-se o delito previsto no art. 154-A (invasão de dispositivo informático), que poderá ser absorvido por crime mais grave. *Exemplo análogo:* agente que joga pedras no portão da vítima, que, ao abrir, é surpreendida com a invasão, ou, ainda, ao abrir, permite que alguém acesse o interior de sua casa.

d) *Phishing scam* (*keylogger* ou captura de dados e atividades feitas) – A vítima recebe e executa um arquivo, mas este não abre portas do dispositivo ou mesmo permite que o atacante o acesse indevidamente. Nesse caso, simplesmente o código captura as teclas digitadas, arquivos pessoais, *sites* acessados ou outras comunicações e envia para o *e-mail*, *FTP* ou servidor do atacante. Logo, não há de se falar em "invasão de dispositivo informático" (art. 154-A), considerando que os dados são remetidos para o atacante e não é o atacante quem os procura, invadindo o dispositivo. Dependendo do caso, poder-se-á tratar a questão como espionagem ou enquadrá-la no conceito de concorrência desleal, prevista no art. 195 da Lei n. 9.279/96. Pode-se pensar no crime de interceptação telemática caso haja interceptação de tráfego (art. 10 da Lei n. 9.296/96). Ainda, pode-se cogitar o delito de furto mediante fraude, considerando o entendimento predominante de que dados e informações poderiam ser furtados.

Exemplo análogo: agente que entrega suposta encomenda para a vítima, que a leva para sua casa, e nessa encomenda existe uma microcâmera que registra as atividades privadas e as encaminha para um receptor ao lado de fora da casa.

Nesse sentido, deve ficar clara a diferença do *phishing* em que ocorre a engenharia social e do *phishing* em que existe o envio de código malicioso. No primeiro, a vítima espontaneamente destravou sua segurança. Já no segundo, sem saber é enganada e sem querer desprotege seu dispositivo informático ou mecanismo de segurança. Ademais, existem modalidades de *phishing* em que sequer ocorre a abertura dos mecanismos de segurança do dispositivo, muito menos invasão, em que informações saem da vítima e vão para o atacante.

Considerar que no *phishing scam* (engenharia social) ocorre a invasão de dispositivo informático (art. 154-A) é assumir a forçosa premissa de que as pessoas são mecanismos de segurança, pois, nesse caso, foram elas as violadas. Isso não é possível para forçar a subsunção ao novo tipo penal.

Tanto é verdade que no Brasil tramita o Projeto de Lei n. 5.485/2013 (disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao ?idProposicao=575520>), que dispõe sobre o "estelionato informático", proposto na Câmara pelo Deputado Eduardo Azeredo, o

qual explica claramente em sua fundamentação que:

Essas novas tecnologias se valem de vulnerabilidades dos navegadores de Internet que permitem o download *e a execução de programas de computador hospedados em* web sites *hostis. Sendo assim, fica evidente a necessidade de uma atualização do Código Penal brasileiro que venha a estabelecer uma tipificação penal relativa ao* phishing*, ou estelionato informático, de forma a desencorajar esse tipo de prática. Uma disposição dessa natureza não foi estabelecida nas recentes legislações editadas sobre o assunto – Lei n. 12.737, de 2012 – conhecida como Lei Carolina Dieckmann, e Lei n. 12.735, de 2012. Este Projeto de Lei, portanto, introduz no Código Penal uma tipificação penal específica que tipifica como crime a prática de difusão de mensagens eletrônicas com o intuito de obter dados pessoais, números de cartão de crédito, senhas, usuários de acesso, de forma fraudulenta.*

Pelo projeto percebe-se a extensão do tipo previsto no art. 171 para fazer frente à prática do *phishing* (especificamente na modalidade engenharia social), vejamos:

Art. 2º O artigo 171 do Decreto Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido do inciso VII, com a seguinte redação:

"Estelionato informático

Art.171. ....

§ 2º Nas mesmas penas incorre quem:

....

VII – envia mensagens digitais de qualquer espécie, fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso".

Não bastasse a assertiva que justifica nosso entendimento de que a Lei Carolina Dieckmann não faz frente ao *phishing scam* na modalidade engenharia social, cite-se recente relatório e versão final do PLS n. 236/2012 (Novo Código Penal), publicado em dezembro de 2014 no Senado, e que contempla

dois tipos penais destinados a fazer frente, especificamente, a essa prática. Vejamos:

PLS 232 Fraude informatizada

Art. 215. Obter, para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução, alteração, supressão ou captura de dados informatizados, ou pela interferência indevida, por qualquer outra forma, no funcionamento de sistema informatizado:

Pena – de prisão, de um a cinco anos.

Parágrafo único. A pena aumenta-se de um terço se o agente se vale de nome falso ou utiliza identidade de terceiros para a prática do crime.

Obtenção indevida de credenciais de acesso

Art. 216. Adquirir, obter ou receber indevidamente credenciais de acesso a sistema informatizado:

Pena – prisão, de um a três anos.

Parágrafo único. Aumenta-se a pena de um a dois terços se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

9.5. Obtenção do conteúdo das comunicações: a divulgação ou comercialização indevida das informações obtidas pode caracterizar outro crime

No delito do art. 154-A do Código Penal, encontra-se a qualificadora do § 3º, que estabelece: se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, haverá uma pena de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (invasão qualificada).

Importante mencionar que não se trata de interceptação de comunicações em andamento, mas do acesso a comunicações armazenadas em dispositivo invadido (como os registros de um *chat* ou mensagens de *e-mails* enviadas e recebidas).

Nestas hipóteses, estabelece o § 4º do precitado tipo penal que se aumenta a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

Esta causa de aumento do § 4º, em tese, pode se incompatibilizar com o conceito trazido pela Lei n. 9.279/96 (Lei de Propriedade Intelectual), que assim estabelece:

Art. 195. Comete crime de concorrência desleal quem:

(...)

XI – divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII – divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude;

(...)

Assim, quando, após a invasão, o agente obter dados ou informações e os divulgar, será preciso ao operador do Direito da Informática avaliar se tratam tais dados ou informações de “informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços”. Nestes casos, não haverá que se cogitar na causa de aumento do art. 154-A do Código Penal, mas sim na incidência do crime de concorrência desleal (art. 195 da Lei n. 9.279/96), cuja pena é de detenção, de 3 (três) meses a 1 (um) ano, ou multa.

9.6. Da causa de aumento se no crime de invasão de dispositivo informático a

vítima experimenta prejuízo econômico

Dispõe o § 2º do art. 154 do Código Penal que se aumenta a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Tal hipótese se configura quando, por exemplo, um dano ao dispositivo for ocasionado por conta do acesso indevido (invasão), ou mesmo nas hipóteses em que o dispositivo precisar ser reprogramado ou enviado ao conserto. Outra hipótese de dano pode ocorrer, por exemplo, quando os sistemas que o dispositivo suportava ficarem indisponíveis, causando prejuízos, inclusive contratuais.

Bem diferente é o dano causado pelos dados que o agente criminoso obtém. Se da invasão, atos decorrentes resultam em um tipo penal, este deve incidir. Como exemplo, a invasão onde o agente consegue dados bancários e desfalca valores da vítima. Em tal situação, não se aplica a causa de aumento do § 2º do art. 154-A do Código Penal, mas, em verdade, estamos diante de um delito próprio, no caso, o furto (art. 155 do Código Penal).

9.7. O art. 154-A como infração de menor potencial ofensivo

O art. 154-A, *caput*, é crime de menor potencial ofensivo, afeto aos Juizados Especiais Federais (art. 61 da Lei n. 9.099/95). Resta evidente que o termo circunstanciado não será suficiente para apuração da autoria em delitos dessa natureza, onde o inquérito policial necessariamente deverá ser instaurado e reputa-se fundamental. Já a prática dos delitos previstos nos §§ 3º e 4º do art. 154-A afasta a possibilidade da competência dos Juizados Especiais Federais, considerando as penas cominadas.

9.8. Do profissional de segurança e a conduta de oferecer ou difundir dispositivo ou programa de computador com o intuito de permitir a invasão

O § 1º do art. 154-A do Código Penal, nos termos da Lei n. 12.737/2012, dispõe que na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a realização da conduta definida no *caput*.

A questão é por demais polêmica e controversa, considerando que pesquisadores de segurança, hoje, desenvolvem e difundem diariamente programas que permitem a “invasão” de dispositivos informáticos. Tais aplicações são divulgadas para finalidades de pesquisa ou mesmo para avaliação da segurança de redes e sistemas.

Sistemas operacionais, como BackTrack, Kali (Linux), são comumente utilizados por profissionais de segurança para realização de testes de intrusão. Outros *frameworks*, como o Metasploit, permitem que o profissional desenvolva um *exploit* para determinada vulnerabilidade a ser explorada. Por sua vez, o programa *sqlmap* é um dos mais utilizados para avaliar a segurança de bancos de dados, realiza diversos testes em bancos de dados de *websites*, permitindo desde o acesso aos registros de um banco, até mesmo a inserção (*injection*) de novas informações.

Como criminalizar todos os profissionais que diariamente manipulam (oferecem, distribuem, vendem ou difundem) estas e outras ferramentas ou *scripts* que permitem a invasão? Tais ferramentas são utilizadas para implementar e testar a segurança da informação, mas também podem ser utilizadas para finalidades maliciosas, assim como uma faca, que pode ser útil na cozinha, mas também ser usada para ferir e matar.

Deste modo, ainda que mediante perícia se possa avaliar se a intenção de um agente, que usa uma das ferramentas comumente usadas por profissionais de segurança, criminalizar a difusão de tais ferramentas pode resultar em graves injustiças.

Isto porque a intenção do agente ao divulgá-las pode ser expor a vulnerabilidade de um sistema, proteger dados dos cidadãos, ou mesmo contribuir para o aprimoramento da segurança, para a comunidade, e não munir bandidos para a prática de crimes digitais. Logo, este difusor não poderia, em tese, responder pelo delito do § 1º do art. 154-A do Código Penal. Neste contexto, ressalte-se

importante reflexão de Amaro Moraes e Silva Neto (2001), a seguir descrita: *"*Se ao caminhar pelas ruas, uma pessoa avistar que os cordões de seus sapatos estão desamarrados, ser-lhe-á devido um agradecimento ou uma censura por se intrometer em sua vida, em sua privacidade? Caso lhe comuniquem que um certo restaurante já provocou intoxicações sérias em diversos incautos que experimentaram suas especialidades, julgaria prudente ir lá e fazer uma refeição e se arriscar a uma desagradável e involuntária ginástica para seus intestinos. Pois bem, no ciberespaço, assim como no Mundo Físico, também existem boas almas que nos alertam sobre os perigos que enfrentamos neste recanto não espacial: são os *hackers* (e, em algumas vezes, até mesmo os *crackers*). São eles que nos sinalizam quanto a similares riscos neste Mundo que não podemos pegar, porque verificaram as debilidades e fragilidades do sistema que os suporta".

Bem diferente é o exemplo do difusor que, ao liberar um programa, faz menção expressa de que está disponibilizando para que seja utilizado para práticas criminosas. Neste caso, é possível identificar, ao homem médio, a intenção daquele que difunde as ferramentas. Como precaução, programadores, *hackers* e profissionais de segurança deverão fazer menção expressa de que estão divulgando determinado dispositivo ou programa para finalidades lícitas, educacionais ou de pesquisa, manifestando expressamente a intenção não criminosa.

Por outro lado, para determinados programas, nem mesmo a manifestação do divulgador de que "não deve ser utilizado com finalidade criminosa" afastará a possibilidade do mesmo ser punido pelo crime do § 2º do art. 154-A. É o caso, por exemplo, do agente que disponibiliza um código malicioso (*Keylogger*) para correntistas de determinado banco. Neste caso, forçoso não concluir que a venda do programa (*trojan*) esteja ocorrendo com a finalidade ilícita de abastecer criminosos digitais.

Uma situação são ferramentas de *pentest* disponibilizadas para *download*, ou mesmo ferramentas para acesso remoto como VNC, Blurp, Team Viewer e Logmein. Outra, "bem diferente", são *trojans*, vírus ou *worms*, como BackOffice, ProRat, ou códigos destinados a alvos específicos, como, por

exemplo, correntistas do Banco A, ou B, ou mesmo programas que permitem destravar proteções autorais ou criptografia de dispositivos (como, por exemplo, TV a cabo).

Como exemplo, aquele que disponibiliza instrumento ou qualquer objeto especialmente destinado à falsificação de moeda (art. 291 do Código Penal), não pode alegar que disponibiliza com finalidades de pesquisa ou para assegurar a segurança da Casa da Moeda. Do mesmo modo, daquele que disponibiliza objeto destinado à falsificação de documentos públicos (art. 294) não seria coerente aceitar a justificativa de que assim o fizera para avaliar a segurança do sistema público. São situações em que, ao senso comum, é possível claramente visualizar a intenção do agente.

Importa dizer, por fim, que nem toda a invasão se dá por meio de programas de computador ou dispositivos. Muitas invasões são exitosas por intermédio de técnicas aplicadas pelos atacantes, muitas vezes, manipulações de dados de programas. Neste cenário, quem divulga técnica ou conceito para invasão, ainda que com fim malicioso, em tese não poderia ser responsabilizado pelo delito do § 2º do art. 154-A do Código Penal.

Isto porque técnica não é um programa e por sua vez uma PoC (prova de conceito) é uma demonstração de como uma invasão ocorreria. Do mesmo modo, vídeos educativos, disponibilizados em canais como Youtube, por exemplo, que ensinam a utilizar determinado programa para "invadir" ou até mesmo determinado *trojan* (cavalo de troia), em nossa visão, não enseja a possibilidade de punição dos publicadores pelo art. 154-A comentado, restando avaliar se é o caso da incidência dos delitos de apologia ou incitação ao crime, previstos, respectivamente, nos arts. 286 e 287 do Código Penal.

Ainda, aquele que disponibiliza uma *webshell* (código que permite administrar um servidor *Web*, se implantado em tal servidor) não pode ser punido por divulgação de programa para invasão, pois embora seja considerada um programa de computador, *shells*, via de regra (poderão existir exceções), são *scripts* utilizados quando a máquina já foi invadida (ou servidores que já estão vulneráveis), e sua função é permitir a administração do servidor ou a prática de outros delitos,

como o dano informático.

9.9. Aquele que acessa indevidamente o computador invadido por outrem

A lei, como redigida, não alcançará os que entrarem em um dispositivo por meio da invasão (ou destravamento de segurança) obtida por um terceiro. Em uma perícia computacional, o perito digital poderá precisar o agente que invadiu e, em ordem cronológica, os IPs (endereços) dos demais que acessaram posteriormente a invasão.

Neste sentido, os demais agentes não invadiram, considerando que o sistema já se encontrava sem mecanismo de segurança ou com mecanismo desativado. Em nossa ótica, é preciso avaliar qual a relação do invasor com os que o sucederam acessando o dispositivo. Ciente da brecha legal, o crime organizado poderá solicitar a um "laranja" localizado no exterior que proceda com a invasão, para que os demais, em território nacional, acessem e obtenham ou alterem as informações. Poderá, no caso concreto, ser apurada a formação de quadrilha ou bando (art. 288 do CP).

Podemos aqui fazer uma analogia com o crime de invasão de domicílio (art. 150 do Código Penal). Mesmo que a casa esteja com as portas abertas, não significa dizer que quem entrar não responderá pelo delito (o que vale é a autorização e não os mecanismos de segurança ativados). Mas, parece que, com os dispositivos informáticos, o raciocínio legislativo foi diverso e, diga-se, equivocado. Imagine um *firewall* que é desabilitado momentaneamente. A proteção existia, mas não estava ativada. Qualquer invasão neste exato momento (datas, horas e fuso horário apuradas por perícia) será conduta atípica, não havendo que se falar em crime.

Sobre este ponto esclarece Cabette (2013, p. 2) o que poderia ser a solução para esta lacuna: "Na realidade o ideal, conforme já dito, seria que o legislador incriminasse diretamente somente a invasão ou instalação de vulnerabilidades, independentemente da violação de mecanismo de segurança. Poderia inclusive o legislador criar uma qualificadora ou uma causa especial de aumento de pena para o caso de a invasão se dar com a violação de mecanismo de segurança. O desvalor da

ação nesse caso seria justificadamente exacerbado, como ocorre, por exemplo, no caso de furto qualificado por rompimento de obstáculo à subtração da coisa".

9.10. A questão do *honeypot*, flagrante preparado e o crime impossível

Honeypots (em português, potes de mel) são mecanismos e recursos computacionais dedicados a ser atacados, sondados ou comprometidos. *Honeynet,* por sua vez, é nome que se designa um tipo de *honeypot*. Por meio de sistemas com HoneyD[84] é possível criar *hosts* virtuais em uma rede, configurados para rodar serviços arbitrários e "chamativos".

A ideia do *honeypot* é prover mecanismos para detectar e avaliar ameaças, sem que estas comprometam os ativos reais. Por intermédio de um *Honeypot*, é possível obter informações de invasores, eis que tão logo comprometida, permite gerar informações sobre o comportamento de um invasor, esteja ele onde estiver.

Embora não possam ser considerados como substitutos de outras ferramentas, como boas práticas de segurança, *firewall*, *intrusion detection system* (IDS), ou sistema de gerenciamento de correções de segurança (*patches*), em verdade, *honeypots* são considerados complementos de segurança em empresas que lidam com dados informatizados.

No Brasil, desde 2008 o projeto Honeynet.br não é atualizado, mas o *site* permanece no ar por motivos históricos[85]. Pode-se aplicar um *honeypot*, por exemplo, dividindo-se o mesmo em três máquinas, uma capturando todos os dados de entrada e saída, a segunda capturando todos os dados do *honeypot*, e a terceira, dedicada à computação forense.

Assim, *honeypots* são uma espécie de armadilha para invasores, pois simulam recursos comprometidos que atraem as "abelhas" e, ao mesmo tempo, coletam informações sobre os mesmos. Com *honeypot*, podemos simular serviços falsos como *smtp*, *FTP*, *web*, com uma senha "fácil" de ser crackeada, permitindo então que vejamos quem são os atacantes e seu *modus operandi.*

Quando um *cracker* varrer a rede, sua atenção será direcionada para o *honeypot*. Sob o prisma

jurídico, esta armadilha seria legal? Poder-se-ia punir o invasor por tê-lo seduzido a praticar uma invasão?

Órgãos policiais poderiam criar *honeypots* para atrair criminosos. Poderiam colocar arquivos protegidos por direito autoral em um *FTP*, com uma senha padrão, "convidando" o acesso de terceiros. Estas pessoas poderiam ser punidas?

Vale lembrar, na Europa, a agência de segurança *European Union Agency for Network and Information Security* (ENISA), que estimula o uso de *HoneyPot* para a caçada de cibercriminosos[86].

No Brasil, essa armadilha poderia ser caracterizada como "crime impossível" ou mesmo "flagrante preparado", e no já fixado entendimento do Superior Tribunal de Justiça, o flagrante preparado, "quando a polícia provoca a pessoa a praticar um crime e, simultaneamente, impede que o delito seja cometido, é ilegal, mas o esperado é regular". Do mesmo modo, o Supremo Tribunal Federal fixou, em 13 de dezembro de 1963, a Súmula 145, que reza: *Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação*[87].

Cumpre destacar que o flagrante digital esperado é possível e não afasta o crime, pois neste, ao contrário do preparado, a autoridade policial se limita a aguardar o momento da prática do delito. Assim, não há crime diante do flagrante preparado, onde o agente é induzido à prática do delito por um agente provocador.

Ademais, ainda que descaracterizássemos a condição da flagrância informática preparada na utilização de *honeypots*, poder-se-ia abordar a questão do crime impossível (art. 17 do Código Penal), isto porque no caso dos *honeypots*, muitas vezes (mas nem sempre, e cada caso deverá ser comprovado pericialmente) não se está acessando um real dispositivo informático da vítima, dados reais, mas uma mera simulação, uma armadilha. Ninguém poderia, em tese, ser punido porque acessou um simulador de dispositivo ou dados fictícios.

Desmerece, em síntese, ser confundida entre *Honeypot* e DMZ (Zona Desmilitarizada), pois nesta existe realmente um ativo da empresa, diga-se, uma rede situada entre uma rede não confiável e outra

confiável. O objetivo é prover uma camada adicional de segurança, onde podem ser instalados filtros responsáveis por realizar o controle do acesso do que entra e do que sai de uma DMZ. As DMZs podem ter a capacidade de conter um ataque ou mesmo minimizar os danos de uma rede.

A invasão frustrada a um dispositivo informático alheio, que é contida ou detectada em uma DMZ, pode configurar o delito do art. 154-A do Código Penal (invasão de dispositivo informático), na sua modalidade tentada. Em que pese, no caso de um ataque a uma rede com DMZ, o invasor não poder acessar a rede privada, é fato que acessará serviços reais da empresa, que estavam na segunda rede, na DMZ que impediu o escalonamento de privilégios e a ampliação do dano.

De outra ordem, ainda, faz-se importante tecer algumas considerações em relação a computadores denominados "zumbis", em que *crackers* podem infectar computadores de civis e, remotamente, disparar ordem para que estes pratiquem delitos ou invadam outros computadores, garantindo de certo modo o anonimato do mandante do crime, também conhecido como *handler*.

Nestes casos, a perícia digital provavelmente chegará até o IP (*Internet Protocol*) do dispositivo "zumbi", muitas vezes de propriedade de uma pessoa que sequer sabia do ocorrido, mas sim teve inadvertidamente seu computador tomado pela ação de um cibercriminoso. Redes com mais de 100.000 computadores já foram detectadas nos Estados Unidos sob o comando de um único criminoso[88].

Logicamente que cuidados medianos devem ser tomados por todos os cidadãos com um computador plugado na rede, como não utilizar *softwares* piratas, manter sistemas de correção atualizados (*patches*) e possuir um bom antivírus, mas, sobretudo, ter cuidado onde clica e evitar a curiosidade excessiva. O titular de uma máquina "zumbi", usada para um crime digital, que comprovadamente por perícia não utilizava nenhuma das medidas acima estabelecidas, certamente assumiu o risco de sua atividade, e pode até vir a ser responsabilizado. Embora não tenha culpa, o usuário pode vir a ter que se explicar em um inquérito ou processo judicial, diante de tamanha desídia para com a proteção de seus ativos informáticos.

Neste sentido, segundo Douglas Wallace (2006, p. 1), “nos Estados Unidos o dono de um computador que fica desprotegido pode até ser preso por negligência. É o mesmo que deixar uma arma carregada em cima da mesa”.

Por outro lado, comprovando-se que o agente titular do “zumbi” não conhecia que estava sendo recrutado para o crime, não pode este responder pelo delito/invasão cometida pelo atacante (*handler*). Isto porque em nenhum momento deu início à execução para invasão da vítima, aliás sequer sabia, tendo sido seu computador que automaticamente respondeu ao comando remoto do criminoso, de forma transparente ao titular do ativo. Logo, é o administrador dos “zumbis” que deve ser identificado e, se for o caso, considerado responsável.

Cada caso concreto deverá ser analisado por perito, para se avaliar se efetivamente o titular do “zumbi” desconhecia ou tinha condições de visualizar a utilização de seu ativo para o crime, dadas as circunstâncias. Se o titular do “zumbi” agiu com culpa, não há concorrência culposa em crime doloso. De outra ordem, caso comprovado o conluio, segue-se a regra clássica penal brasileira. Neste sentido, dispõe o art. 29 do Código Penal:

Art. 29. Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade.

§ 1º Se a participação for de menor importância, a pena pode ser diminuída de um sexto a um terço.

§ 2º Se algum dos concorrentes quis participar de crime menos grave, ser-lhe-á aplicada a pena deste; essa pena será aumentada até metade, na hipótese de ter sido previsível o resultado mais grave.

Bem diferente, também, é o caso do usuário que voluntariamente alista sua máquina para ser um “zumbi” de um criminoso digital. Como, por exemplo, *download* voluntário e configuração da aplicação LOIC, um programa de código aberto que tem o objetivo de executar ataques de negação de serviços, desenvolvido em C#. Assim, com o LOIC, é possível deixar uma máquina pré-

configurada para ser um “zumbi”, que pode ser usada para ciberativismo sim (atividades licitas), mas também para a prática de crimes digitais.

Tais ferramentas dificultam igualmente a análise pericial, pois segundo Milagre (2011, p. 1), “a despeito das opiniões daqueles que entendem que usuários podem ser considerados partícipes ou coautores de ataques digitais (considerando o dolo e a potencial consciência do caráter ilícito do fato), o fato é que estamos diante de um desafio, eis que os *crackers* já encorajam usuários a alistarem suas máquinas, alegando a estes que se forem pegos, basta sustentar a tese que o computador foi infectado por um vírus e que nada sabem a respeito”.

9.11. A teoria da imputação objetiva e a autocolocação em risco da vítima de crime cibernético

A autocolocação da vítima em risco importaria, em tese, excludente da tipicidade do fato, logo, eximiria a responsabilidade criminal. Vejamos as circunstâncias em que alguém se coloca em situação de perigo ou mesmo se expõe a um perigo já existente.

A autocolocação em risco ocorrerá sempre que a vítima, de modo consciente ou não, contribuir com sua conduta para o resultado do delito. Esta conduta da vítima pode se dar concomitantemente à ação do partícipe ou mesmo posteriormente a esta.

E como a vítima pode ser partícipe do crime cibernético?

Viver na sociedade da informação é muito perigoso. Como ficaria o caso do usuário que não coloca senha em seus dispositivos, ou que usa senha fraca? Ou mesmo do usuário que clica em tudo que vê? Ou ainda do cidadão que não adota antivírus em seu ativo ou anda com sistema operacional mais que desatualizado?

De maneira que só podemos cogitar em imputação penal a alguém, se da conduta deste agente adveio resultado ou risco juridicamente desaprovado e não permitido pela sociedade. No âmbito da imputação objetiva poder-se-ia cogitar do critério da diminuição do risco, nos casos de alguém que

não criou o risco, mas tenta diminuí-lo, causando um resultado lesivo.

Tomemos o exemplo de agente que interrompe um serviço informático para evitar um acesso indevido que estava em andamento, ou mesmo que, para evitar eventual acesso indevido a informações, apaga dados pertencentes a outrem, ou mesmo a hipótese do agente que acessa indevidamente um dispositivo informático alheio para protegê-lo de um ataque, corrigir uma vulnerabilidade ou mesmo eliminar um *malware* instalado.

Deve-se considerar, também, analisando condutas informáticas, o critério da proibição de regresso, onde uma pessoa, por uma conduta inócua anterior à prática do delito ou a uma conduta criminosa, não poderia ser considerada coautora do crime. Um exemplo é o agente que apenas infecta a vítima, tornando sua máquina vulnerável, para que outra pessoa explore e pratique a invasão.

Ainda, em se tratando de imputação objetiva, um dos critérios que podem ser considerados é a teoria do âmbito de proteção da norma. Por tal teoria, sempre que uma conduta ocasionar dois riscos, um relativo à própria conduta e outro relativo ao perigo geral, o agente só será responsabilizado pelo resultado advindo à vítima de sua própria conduta. Como exemplo, citamos o agente que interrompe serviço telemático de uma pessoa. Da interrupção, clientes da vítima também experimentaram falhas em seus sistemas. O *cracker*, em tese, responderia pela indisponibilização do serviço em que atuou. Outro exemplo, o sujeito que comete uma invasão em banco de dados de um setor financeiro e lá altera informações. Investidores influenciados podem ser coagidos a manipular erroneamente seus investimentos.

Por outro lado, em se tratando da autocolocação da vítima em risco, temos algumas considerações em relação a crimes de informática. Alguns casos que poderiam ser considerados (refletidos) são:

• vítima de invasão que fora alertada anteriormente sobre a vulnerabilidade e nada fizera;

• vítima de invasão de dispositivo informático que, mediante perícia, restar comprovado ter utilizado *hotspot* público e sem proteção;

• vítima que mantinha uma senha como 12345, internet, ou admin, senhas facilmente descobertas;

• vítima que tinha em seu computador sistema operacional pirata ou desatualizado;

• usuário que acessa serviço bancário sem adotar medidas de segurança;

• vítima que acessa *sites* suspeitos, redes não protegidas ou mesmo não adota *firewall* ou qualquer mecanismo de segurança.

Deve-se destacar, todavia, que, embora tenha surgido de um julgamento de um Tribunal alemão, a teoria da autocolocação da vítima em risco já foi reconhecida em alguns casos pontuais no Brasil.

Neste cenário valem os ensinamentos de Marcelo Xavier de Freitas Crespo (2011, p. 108), que, ao tratar da temática em estudo, assim pontua: "Como conclusão, tem-se que quanto maior a educação dos usuários dos computadores, menores as chances de os criminosos se locupletarem das situações de risco criadas pela atual sociedade global do risco informático e da informação. Porém, ao mesmo tempo, há mais subsídios para excluir-se ou diminuir sua responsabilidade penal devido ao amadurecimento e conhecimento por parte dos usuários dos riscos inerentes ao uso da Informação nos dias atuais".

A esse respeito, em julgado sobre o tema, no qual correntista buscava na seara cível reparação de danos por fraude bancária, assim entendeu o TJSP, ao absolver o banco de qualquer responsabilidade:

DANO MORAL. Responsabilidade Civil. Senhas e acesso ao sistema bankline *– Pretensão do banco réu de reformar sentença que julgou procedente pedido de indenização por danos morais sofridos pelo autor pela má prestação de serviços. Cabimento. Hipótese em que os transtornos aos quais o autor foi submetido, com o débito indevido de valores da sua conta corrente, não configuram dano moral, uma vez que o próprio autor foi negligente no acesso ao sistema informatizado. RECURSO PROVIDO.PEDIDO DE REPETIÇÃO DE INDÉBITO. Pretensão de reforma da sentença que julgou procedente pedido de repetição de indébito. Descabimento. Hipótese em que os valores cobrados eram devidos. RECURSO PROVIDO. DANO MATERIAL. Pretensão de reforma da sentença que condenou o apelante ao pagamento de danos materiais por*

saques e pagamentos indevidos efetuados na conta do apelado. Cabimento. Hipótese em que o dano patrimonial foi causado por culpa exclusiva do autor. RECURSO PROVIDO (TJSP – APL: 158732420078260510 SP 0015873-24.2007.8.26.0510, Rel. Ana de Lourdes Coutinho Silva, j. 27-7-2011, 13ª Câmara de Direito Privado, *DJ* 2-8-2011).

9.12. A invasão de dispositivo informático e o *Drive-by-Download*

Denomina-se *Drive-by-Download* o processo onde um *software* ou código malicioso é baixado e por vezes instalado automaticamente no computador do usuário, sem o consentimento do mesmo.

Normalmente, a infecção ocorre por meio do acesso a *site* onde ocorre execução de arquivo camuflado de uma aplicação convencional (mascarando, por exemplo, a atualização de um *plug-in* supostamente necessário para acesso ao *site*), muitas vezes executado via Java Applet, que, na grande maioria das vezes, infecta o usuário, que executa a aplicação “clicando em Run”[89].

Em algumas situações (dependendo da configuração do *browser*), basta o acesso ao *site* para que o código malicioso seja acessado e o arquivo copiado para o computador do usuário (*malware*). Este arquivo pode, desde garantir o acesso e o controle do equipamento infectado, a copiar ou destruir dados existentes na máquina da vítima.

Neste caso, a infecção via ação direta por ação do agente criminoso, como, por exemplo, ao enviar um *e-mail* para a vítima com o código malicioso, poderia ser classificada como furto mediante fraude (art. 155, § 4º, II, do Código Penal), na medida em que o agente, se consumado o delito, obtém vantagem financeira, induzindo a vítima em erro e subtraindo valores de sua conta bancária. Para alguns autores, caso não haja o furto, já estaria caracterizado o delito de invasão de dispositivo informático (art. 154-A do Código Penal), pois segundo estes e como já mencionado no livro, a fraude seria o caminho para a invasão. A este respeito, ver nosso entendimento nas p. 107 e 127 e seguintes deste livro, exemplificado no caso de *phishing scam*, em que propomos um quadro elucidativo.

Sob outro prisma, no caso do *Drive-by-Download*, muitas vezes é a vítima que voluntariamente acessa determinado *site* e lá, também voluntariamente, executa ou confirma alguma *dialog box*, que promove a infecção com o código malicioso. A partir daí, seu computador pode ser acessado, à medida que são quebrados os mecanismos de segurança.

Se comprovado por perícia que o *site* foi dolosamente hospedado por criminoso, este pode responder pelo delito de furto mediante fraude, caso o agente tenha obtido vantagem da conduta, subtraído a coisa (comumente, valores da conta bancária da vítima). Por outro lado, muitos *sites* por vezes são usados por criminosos digitais como "hospedeiros" de códigos *Drive-by-Download*. Nesta hipótese, deve-se apurar se o titular do *site* (hospedagem) tinha conhecimento da existência do código ou não, antes de se pensar em responsabilização do mesmo, nos termos do art. 29 do Código Penal.

Se não tiver conhecimento de que seu *site* servia ao crime digital, não existe dolo e, logicamente, o titular do *site* não poderá ser responsabilizado. Sem prejuízo, poderá o titular do *site* eventualmente responsabilizar o atacante por violação de dispositivo informático, tendo em vista a implantação de um *malware* em seu *website* (fazendo-o servir como arma para o crime cibernético). Deverá provar que o *site* invadido estava protegido com mecanismo de segurança (servidor *Web* atualizado, IDS, proteção de permissões nas pastas do *FTP*, Firewall, ou proteção minimamente aceitável), pois, do contrário, feita a auditoria de código-fonte, não caracterizará a invasão (a perícia digital é instrumento que poderá afirmar se o mecanismo de controle era efetivo ou não).

Resta saber se a vítima que voluntariamente acessa um *site* e, sem saber, executa código que instala arquivo malicioso, abrindo as portas de sua máquina para o acesso indevido, e diante do acesso tem valores furtados, pode ser vítima do delito previsto no art. 154-A do Código Penal, de acordo com a Lei n. 12.737/2012 (invasão de dispositivo informático) ou seria o caso da aplicação do delito do art. 155, § 4º, II, do Código Penal (furto mediante fraude), considerando que não houve ato comissivo (ativo) de "invasão", mas tão somente execução de uma aplicação que liberou as portas do

computador para ser acessado? Soma-se a esta complexa questão o fato de que, em alguns casos, o código malicioso instalado no computador da vítima executa o que nominamos de *connection back*, ou seja, é a máquina da vítima que se conecta no computador do *cracker* e este, então, tem acesso ao conteúdo do computador daquela.

Analisemos o contexto: agente que hospeda código malicioso em um *site*, código este que permite o envio de arquivo ou execução de código que abre as portas da máquina da vítima, quando esta acessa a página, permitindo a conexão remota a sua aparelhagem. A vítima é motivada, então, a acessar o *site*, infectando-se. O agente, então, acessa indevidamente o computador da vítima, obtendo informações e tendo vantagem nas informações acessadas, como, por exemplo, *desfalque bancário na conta da vítima.*

Há várias condutas no exemplo acima, como o preparo do *site* com código malicioso, e a programação do *malware* que é instalado no computador da vítima, liberando as portas da máquina para conexão remota. Logicamente, ao liberar portas que estavam fechadas, nitidamente o agente está "violando indevidamente mecanismo de segurança", para posteriormente acessar indevidamente o conteúdo e ter acesso a informações que lhe proporcionarão vantagem (saques bancários).

Sob outro prisma, percebe-se que a invasão (art. 154-A do Código Penal), neste caso, é conduta-meio para a prática do delito-fim, ou seja, para que o agente "subtraia a coisa" é importante que primeiramente induza a vítima em erro com o código malicioso e que depois acesse indevidamente o dispositivo informático da vítima (conduta afeta ao delito de invasão de dispositivo informático), tendo acesso a informações que lhe permitam subtrair o bem da vítima, protegido pelo Direito Penal.

Neste sentido, exemplifica Guilherme da Rocha Ramos (2000, p. 4) que "no entanto, se digo que o agente A, com o intuito de furtar bens de uma residência, escala o muro que a cerca e, utilizando-se de chave falsa, abre-lhe a porta e penetra no seu interior, subtraindo-lhe os bens e fugindo logo em seguida, posso com toda a certeza afirmar que o princípio da consunção se faz presente: o crime consuntivo (que é sempre mais grave que os consuntos), i. e., o furto qualificado pela escalada e pelo

emprego de chave falsa (art. 155, § 4º, II, 3ª figura, e III, do Código Penal) absorve o consunto, vale dizer, a violação de domicílio qualificada (art. 150, § 1º, 1ª figura, do Código Penal), que lhe serviu de meio ou fase executória necessário(a)".

Com efeito, pelo princípio da consunção, o delito de furto mediante fraude, com pena mais grave, previsto no art. 155, § 4º, II, do Código Penal, absorveria, via de regra, o delito do art. 154-A do Código Penal, nos termos da "Lei Carolina Dieckmann" (invasão de dispositivo informático), no exemplo dado acima, envolvendo um ataque via *Drive-by-Download*, se efetivamente houve o desfalque financeiro da vítima.

Sob outro aspecto, outras questões devem ser consideradas. Existem situações em que o ataque ora analisado pode ser *auto-infect*, ou seja, sem interação do alvo. Diga-se, basta à vítima acessar um *site* para que fique infectada com o *malware* (código malicioso). A vítima não precisa clicar em nada. Sequer sabe que está sendo infectada.

Estamos diante de uma situação onde o atacante não tem vítima certa e determinada (como no caso dos ataques APT – *Advanced Persistent Threat*), mas lança o *site* no ar, com o código malicioso, para lesar "vítimas incertas e indeterminadas", diga-se, quem acessar o portal será infectado. Neste exemplo, o agente criminoso não induz a vítima a acessar o *site*, com uma mensagem ou *e-mail*. Tão somente hospeda o *site*, aguardando vítimas "entrarem", "caírem na rede".

Quando a vítima acessa, é infectada e então permite o acesso indevido ao seu dispositivo pelo criminoso, que captura informações que utilizará para o dano ao patrimônio. Se o agente descobrir que foi vítima, pode registrar ocorrência ou requerer instauração de inquérito policial por furto mediante fraude. Porém, pode ser que alguém descubra o *site* criminoso no ar e encaminhe para as autoridades, sendo que delegado de polícia ou promotor de justiça não conhecem o autor do golpe e vítimas que eventualmente já foram lesadas. Nesta hipótese, ainda que se apure a autoria e o dolo do titular do *site*, não poderá a autoridade precisar as vítimas do crime, considerando que as mesmas são incertas.

Deste modo, tem-se que o crime de furto mediante fraude deve atingir pessoas ou vítimas certas. Em caso de vítimas incertas, a conduta poderá se enquadrar no conceito do crime contra a economia popular.

Assim dispõe a Lei n. 1.521/51: *Art. 2º São crimes desta natureza: (...) IX – obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve", "cadeias", "pichardismo" e quaisquer outros equivalentes).*

Logo, um promotor que descobre um *site* no ar que está distribuindo *malware* para quem acessa, via de regra, não poderia processar o autor por furto mediante fraude, sem antes apurar se o mesmo obteve a coisa alheia e, principalmente, quem foram as vítimas. No máximo, pelo *site* que está no ar pode responsabilizar, de plano, o autor, pelo delito envolvendo crime contra a economia popular.

De outra ordem, pode ser que o código malicioso hospedado no *site* do atacante não permita a subtração de dados bancários, mas tão somente o acesso a informações diversas da vítima. Neste caso (embora frisemos, existem divergências de entendimentos), o delito é o do art. 154-A do Código Penal (invasão de dispositivo informático), e não o furto mediante fraude.

É possível cogitar-se, ainda, da situação onde o código malicioso sequer permite a invasão, ou a coleta de dados financeiros, mas tão somente faz com que a máquina vire um *pivot* para, por exemplo, atacar outro serviço. Neste caso, não havendo invasão, nem furto mediante fraude, e desconhecendo a vítima que sua máquina era um "zumbi", só responderá o autor do comando ou *trojan*, pelo delito que consequentemente corresponder sua conduta em manipulação à máquina de terceiros, a partir do "zumbi", sendo que da simples invasão destas máquinas, se dolosa, responderá pelo delito do art. 154-A do Código Penal.

Pode-se cogitar, por fim, da situação em que o *malware* não destravou os mecanismos de segurança da máquina da vítima, mas executou uma "conexão reversa", mandando informações para o atacante (via captura do teclado, por exemplo), informações estas não bancárias, não havendo qualquer

subtração da coisa (dinheiro). Neste caso, não existe furto mediante fraude. Igualmente, via de regra, não haveria de se falar em invasão de dispositivo informático, pois, em tese, foi a vítima que se conectou ao agente criminoso, executando o *malware*, por exemplo, enviado via engenharia social. A questão não é pacífica, pois deve-se considerar que em alguns casos de *connection back*, o código que o realiza foi implantado via invasão ou injeção e não executado pela vítima. Cada caso é um caso.

9.13. Dez vulnerabilidades *web*, críticas e o eventual enquadramento na Lei n. 12.737/2012

É utópico dizer que a "Lei Carolina Dieckmann" resolve o problema do crime digital ou faz frente àqueles que exploram falhas de segurança. São poucas as técnicas ou as condutas que podem ser enquadradas em seu conceito. Em verdade, a violação de computadores pode se dar por meio da exploração das mais variadas falhas.

A *The Open Web Application Security Project (*OWASP) é uma associação mundial que reúne especialistas em segurança *web*. A comunidade desenvolve artigos, metodologias, documentação, ferramentas, bem como trabalha em técnicas e tecnologias para aprimorar a segurança da informação.

A entidade, que não tem fins lucrativos, elabora importantes estudos para aprimoramento da segurança digital em nível global, sendo referência para entidades como *U.S. Defense Information Systems Agency* (DISA), *U.S. Federal Trade Commission* e outras entidades, empresas e organizações em todo o mundo.

Um dos principais trabalhos da OWASP é a chamada lista *The top 10 most critical web application security risks,* reunindo o que se chama de riscos de ataques mais críticos que podem ser aplicados a partir de vulnerabilidades *web*[90]. Passemos a estudar e refletir sobre a última versão dessa lista, consequentemente, à análise de cada risco, de acordo com sua criticidade (grau de severidade).

9.13.1. Injection

Ataques de *injection* (como SQL, OS, LDAP, dentre outros) ocorrem quando um dado não confiável (não tratado ou sanitizado) é enviado a um interpretador como parte de um comando ou *query* (instruções a um banco de dados ou aplicação). Ao alterar ou inserir parâmetros não confiáveis, o atacante pode executar comandos não esperados no servidor, muitas vezes vindo a acessar dados restritos.

Embora ataques de *injection* não aconteçam apenas em aplicações *web*, de um ataque que explora uma vulnerabilidade na aplicação *web* que permite o *injection*, podemos ter uma invasão, ou acesso indevido a um dispositivo informático, com a finalidade mínima de obter informações. Se confirmada a "finalidade dolosa", pode o agente responder pelo delito do art. 154-A do Código Penal, nos termos da Lei n. 12.737/2012. Cada caso concreto deverá ser analisado por peritos e autoridades que contem com profundo embasamento técnico. Conceituar invasão no âmbito de um ataque *sql injection* é extremamente complexo. Pode haver, na análise de casos concretos, obtenção de dados sem invasão.

Como o nome diz, no *injection*, o agente injeta códigos em um sistema e consegue acesso a detalhes do banco de dados. Estes detalhes são dados retornados, podendo ser até mesmo telas de erro, que indicam que um sistema está vulnerável.

É preciso distinguir o acesso ao banco de dados e o acesso a informações que demonstram que um sistema está vulnerável. O agente que introduz uma aspas simples em um campo de um formulário em um *site*, permitindo verificar uma mensagem de erro no banco de dados, em tese, está praticando a tentativa de descobrir uma vulnerabilidade, e não tentativa de invasão em si, esta, punível pelo art. 154-A do Código Penal. Como se verifica, é preciso analisar o *iter criminis* de cada caso concreto, de modo a identificar se a conduta praticada por esta técnica reúne elementos de uma invasão ou não e, se positivo, se a finalidade é a descrita em lei ou não.

Questão que se coloca é se um *site* com uma vulnerabilidade *web* estaria com efetivo mecanismo

de segurança, e se a exploração de uma vulnerabilidade já existente constitui violação indevida a este mecanismo. Como é sabido, para que o agente possa responder pelo crime de invasão de dispositivo informático, é necessário que haja a "violação de mecanismo de segurança".

Para alguns especialistas, se o serviço vulnerável a *injection* estivesse protegido por IPS (*Intrusion Prevention System*) ou WAF (*Web Application Firewall*) e houvesse o *by-pass*, aí sim, estaríamos diante da "violação de mecanismo de segurança". Acrescente-se ainda que falhas que permitem *injection* são consideradas, via de regra, de fácil exploitabilidade (exploração pelo atacante), logo, não seria qualquer dispositivo ou sistema explorado via *injection* que mereceria a proteção criminal.

Nesta linha de raciocínio, e para esta corrente, temos que muitas vezes uma aplicação não possui *appliances* de segurança como um IPS (mais voltado para vulnerabilidades de rede) ou WAF e, neste caso, o atacante não estaria realizando qualquer violação. O atacante estaria "apenas" injetando código malicioso a fim de tirar algum proveito das informações que conseguir obter.

No caso, a falha seria a aplicação *web* não ter sido desenvolvida de forma segura, considerando boas práticas de programação, uso de API's seguros, dentre outros. Para tal corrente, "programação segura" seria um mecanismo de segurança. Logo, ao injetar um código em um sistema não protegido por *appliance* ou outro dispositivo, e logrando êxito na injeção do código, o agente não cometeria crime algum, pois o êxito do código aplicado revela a ausência de programação segura, logo, ausência de mecanismo de segurança.

Por outro lado, em que pese seja uma falha de fácil exploração, para outra corrente, o mecanismo de segurança poderá ser provado (por perícia) simplesmente constatando-se a presença de controles mínimos, como a existência de senha para acesso ao banco de dados ou a segurança da própria aplicação (como funções de proteção a *injection* e XSS) de modo que a conduta poderia, se constatada, ser enquadrável no conceito de invasão (logicamente, se comprovada uma das intenções da invasão previstas em lei). Para esta corrente, não se pode transferir ao WAF ou ao IPS a

segurança da aplicação e não há de se perquirir se o *firewall* está ou não bem configurado ou com todos os módulos necessários ativos.

Atente-se que, por falha legislativa, não se vincula necessariamente o “mecanismo de segurança” ao bem protegido, o que pode dar margem a falhas interpretações por parte de autoridades e peritos. Exemplo: um disco rígido que tem senha no sistema operacional, mas é retirado da máquina pelo criminoso e montado em outra máquina como *slave* (escravo) em outra máquina, fazendo com que o agente tenha acesso ao dispositivo sem “violar” mecanismo de segurança.

Tome como exemplo um banco de dados de um serviço *web*, cujo desenvolvedor não implementou uma senha, mas que está hospedado em um *host* com um antivírus. Um perito desorientado, ao responder o quesito ao juiz ou promotor, poderá informar que “sim, o ativo possuía mecanismo de segurança”. Uma falha, pois, embora seja um mecanismo de segurança aplicado ao suporte do ativo, era tal mecanismo, via de regra, ineficaz para proteger o bem jurídico (informações do banco de dados) do ataque aplicado, cujo atacante sequer se deu conta da existência de tal mecanismo, logo, não violando nada.

Para uma terceira corrente, ainda, em qualquer atividade de injeção de códigos em uma aplicação para recuperar dados do banco de dados, ainda que uma simples injeção de uma aspas simples, ocorrerá o *injection* e, consequentemente, invasão, independentemente da segurança empregada na aplicação ou banco de dados. Para esta corrente, a injeção de código foi capaz de fazer um sistema se comportar de modo inesperado, fora do seu comum, revelando dados (ainda que mera mensagem de erro) e violando a “segurança” descrita nos fluxos do sistema. Definitivamente, não aceitamos como a interpretação mais adequada.

A exemplo, um registro:

a) www.meusite.com.br/aplicativo.asp?variavel=;nc 200.200.200.200 10000 -e /bin/bash;

não poderia ser considerado o mesmo que

b) www.meusite.com.br/aplicativo.asp?variavel=’;

ao avaliarmos se o agente invadiu ou não um sistema, e qual sua "intenção".

No segundo exemplo é impossível concluir que a intenção do agente era invadir ou obter informações.

Acrescente-se ainda uma variável. Nem todo o ataque *injection* pode estar sobre um sistema com banco de dados com informações privadas ou confidenciais (como *login* e senha ou ainda dados bancários de usuários).

Um ataque dessa natureza pode se dar, por exemplo, a um banco de dados de notícias, diga-se, informações já conhecidas. Neste caso, o simples acesso, ainda que indevido, às informações diretamente em banco de dados (para mostrar a insegurança), em que pese possa ser considerado crime, não deve ter o mesmo peso, pois o agente simplesmente obteve informações públicas, de outra forma. Por outro lado, ao inserir uma nova notícia, ou se a partir do *injection* consegue alterar, destruir informações, inserir um *backdoor*, poderá ser responsabilizado pelo delito previsto no art. 154-A do Código Penal.

Outra questão que merece reflexão é se o agente, a partir do *injection* a um banco de dados de informações públicas, disparar outros comandos para acessar o servidor, ou seu código disparado em um banco com informações públicas lhe permitir acesso à máquina que hospeda o *website*. Neste caso, o *iter criminis* poderá ser considerado para apurar a invasão à máquina servidora.

Temos, pois, uma segunda conduta do agente, a partir de um primeiro acesso. Diga-se, através da exploração de falha em um *site*, poderá ter acesso a toda a máquina. Embora tenha feito o primeiro acesso a informações públicas (como, por exemplo, banco de dados de notícias), do acesso resultou novo acesso a outro sistema, momento em que forçosamente terá contato com informações privadas, fase em que o crime de invasão de dispositivo informático se consuma. Se as provas demonstrarem que da invasão retornou para o agente apenas a tela do sistema operacional, caberá, na instrução processual, a prova de que tal invasão era com o escopo de obter informações específicas ou não. Uma quesitação importante que a defesa poderá fazer para o perito é: "A máquina invadida

definitivamente possuía informações específicas passíveis de serem obtidas ou adulteradas?". A questão é importante, pois, do *injection*, o agente poderá, em alguns casos, conseguir acesso administrativo, mas não acessar nenhum dado ou informação. Tal fato pode caracterizar ausência da "intenção" de obtenção de dados.

Nesta linha de raciocínio, deve-se advertir, será necessário, sempre, avaliar por meio de perícia o código ou *exploit* utilizado, ou mesmo o parâmetro passado no ataque, para se constatar o que executava e quais informações levantava (a profundidade dos efeitos dos códigos transmitidos). Um exemplo seria o ataque que simplesmente levantou o "nome da base de dados" e foi finalizado. Com certeza, com o nome da base de dados, seria possível levantar as tabelas e por fim os registros. Mas o agente interrompeu a execução. Deveria ser punido? Se sim, por tentativa de invasão ou já pela invasão consumada, considerando, neste caso, que sua conduta comprovaria sua intenção em obter dados? Correntes doutrinárias se dividem a respeito.

Em nossa ótica, a tentativa seria a resposta para o exemplo. Por outro lado, caberá aos operadores do Direito o discernimento entre "tentativa de encontrar vulnerabilidade" e "tentativa de invasão", pois, em muitos casos, a injeção de código pode revelar não o interesse em obter dados, mas de testar a segurança de um sistema, fato atípico. Com efeito, forçoso processar ou punir alguém por invasão de dispositivo informático. A linha é tênue e passa, necessariamente, pela prova pericial.

Assim, a tentativa de invasão pela técnica de *sql injection*, por exemplo, se dará quando o sistema não estava vulnerável, mas as tentativas de acesso às informações ficaram registradas nos *logs* do sistema. Ainda assim, como proposto, caberá ao técnico avaliar os *logs* com cautela, mensurando se realmente demonstram a intenção de obtenção de dados ou de mero teste da segurança em um sistema.

9.13.2. **Broken Autentication and Session Management**

Trata-se de um risco relativo à gestão de sessões e autenticação, onde funções não foram

corretamente implementadas, permitindo que atacantes comprometam senhas, chaves, *tokens* de sessões ou mesmo explorem falhas para assumir outras identidades.

Em um dispositivo com tal risco, tem-se um mecanismo de segurança, porém mal implementado. Como verificado, a legislação sobre invasão de dispositivo informático exige que o dispositivo esteja protegido por "mecanismo de segurança", não exigindo que o mesmo esteja 100% implementado corretamente.

Não se pode desconsiderar a importância da análise pericial, que poderá concluir se a exploração da falha de implementação só poderia ser feita por *cracker*, ou se em verdade a falha correspondia à "inexistência" de proteção para o acesso indevido, permitindo a qualquer um o contato com os dados.

Importa dizer que, para parte dos especialistas, o controle de sessão poderia ser considerado um mecanismo de segurança, como, por exemplo, além da implementação de um forte mecanismo de autenticação (considerando, por exemplo, a autenticação multifator – quem você é, o que você possui, o que você sabe), a implementação de mecanismos de *logs* de usuários (principalmente usuários administrativos) e controle de tempo de sessão (o acesso "cai" após um período de inatividade). Análise pericial será indispensável.

9.13.3. Cross-Site Scripting (XSS)

A falha XSS ocorre quando aplicações aceitam código não confiável (não tratado, sanitizado), que é enviado ao navegador *web* da vítima. Neste cenário permite ao atacante executar *scripts* no navegador da vítima que podem roubar um número de sessão, roubar dados de *cookie*, inserir informações falsas na tela de um usuário ou mesmo redirecionar usuários para *sites* maliciosos.

O enquadramento jurídico da exploração de uma falha dessa natureza é complexo. Primeiramente, temos a conduta inicial envolvendo o envio de código para explorar o navegador do usuário ou aplicações como Java, Flash etc. Comumente, este voluntariamente acessa *link* ou arquivo malicioso

que infecta as bibliotecas do navegador (Reflected XSS). Forçoso se cogitar em tentativa de invasão daquele que disponibiliza código XSS, considerando que a vítima voluntariamente assim acessou o código HTML ou JavaScript, que altera seu próprio navegador, considerando ainda que, a princípio, o XSS não seria usado para invasão. A conduta de enviar *link* malicioso a vítima poderá ser considerada como tentativa de outros crimes, como furto mediante fraude (art. 155, § 4º, do Código Penal) ou estelionato (art. 171 do Código Penal), ou mesmo como fato atípico, quando do acesso a informações da vítima, a partir da técnica empregada, verificou-se não se tratar de dados pessoais ou financeiros ou mesmo quando não houve vantagem indevida.

Na sequência, com o código interpretado pelo navegador, a vítima pode ter, por exemplo, uma identidade visual de um banco falseada em seu navegador, fazendo com que entregue dados bancários para o criminoso, que efetuará o desfalque. Neste caso, estamos diante do delito de furto mediante fraude, previsto no § 4º do art. 155 do Código Penal. O mesmo vale para o código que redireciona o usuário para um *site* malicioso, fazendo com que este forneça dados pessoais.

Outra modalidade do ataque é o Stored XSS, onde a aplicação vulnerável armazena o código no banco de dados e posteriormente exibe para um usuário do *site*. Exemplo: o agente que coloca código em comentários em uma rede social fazendo com que outros visitantes que acessem tenham sua máquina com visual alterado. Neste caso, a vítima não precisou clicar em nada ou acessar *links* com variáveis manipuladas. Ele apenas acessou o *site*.

Com este acesso ao *site*, por exemplo, a vítima pode ter seus *cookies* acessados pelo atacante. Embora o atacante tenha o “acesso indevido” a informações, para uma primeira corrente, forçoso concluir, nesta modalidade, haver invasão punível, mas a questão merecerá maiores reflexões do Judiciário, juntamente com especialistas em segurança.

Pode ser, ainda, que o código XSS sequestre a sessão do usuário, que poderia estar loggado (conectado ao sistema), por exemplo, em um disco virtual ou em seu banco. Nestes casos, uma primeira opinião entende que não haverá invasão de dispositivo informático, pois não aconteceu

"violação indevida de mecanismo de segurança", tendo-se em vista que o usuário já estava registrado no sistema (tinha permissão). Em sentido diverso advogava outra corrente, demonstrando que, embora a vítima tivesse acesso ao sistema acessado indevidamente pelo atacante, a manipulação da vítima demonstra uma destreza absoluta em usá-la como chave para acesso a um dispositivo informático, logo, violando mecanismo de segurança. Ademais, outros crimes poderão advir das condutas do agente criminoso que tem acesso ao conteúdo privado da vítima, conteúdo este que somente esta teria acesso legítimo.

Assim, se da falha XSS o agente atacante consegue acesso à administração de um *site* ou dispositivo, e lá realiza o *defacement*, ou obtém informações, pode-se cogitar da aplicação do delito previsto no art. 154-A do Código Penal.

9.13.4. Insecure Data Object References

Esta falha ocorre quando um administrador ou desenvolvedor expõe referências a um objeto interno como arquivo, diretório, senha do banco de dados, dentre outros. Não implementando controle de acesso, atacantes podem manipular estas referências para acessar dados não autorizados.

Este é o caso do agente que configura erroneamente uma aplicação, oferecendo permissão geral de pastas restritas a usuários, grupos e outros. Ou mesmo o agente que não protege arquivos de conexão com banco de dados referenciados pela aplicação, permitindo que o agente conheça o nome de usuário e senha para acesso ao banco. Outro exemplo que se pode citar é quando o agente acessa, por exemplo, faturas ou pedidos de outros clientes, somente mudando o *id* de controle passado via método GET ou POST, ou ainda nos casos do chamado LFI (*Local File Include*), em que o agente consegue ler o arquivo *config* diretamente, no qual se encontra a senha do banco de dados.

Nestes casos, o criminoso que se vale dessas informações não está invadindo dispositivo informático alheio, pois, via de regra, o acesso a elas foi imprudente ou negligentemente permitido pela própria vítima (ou por quem administra seus ativos). Logo, o agente que obtém senha exposta em

objetos de dados não protegidos, e acessa dispositivo informático, não o está fazendo mediante "rompimento de mecanismo de segurança", uma vez que ele não existe, não havendo que se falar do delito previsto no art. 154-A do Código Penal.

9.13.5. Security Misconfiguration

Falha que envolve genericamente má configuração da segurança definida para dispositivos como *frameworks* de aplicações, servidores de aplicações, servidores *web*, servidores de bancos de dados e plataformas. Inclui os casos envolvendo *softwares* desatualizados.

A questão do "*software* desatualizado" caracterizar ausência de mecanismo de segurança é polêmica. Para parte da doutrina, em uma analogia, o cidadão que usa uma "velha garrucha" para se defender está empregando mecanismo de segurança, ainda que "desatualizado". Logo, se importarmos o pensamento para a informática, deve estar protegido pela Lei n. 12.737/ 2012, a despeito da modernidade ou obsolescência do mecanismo de segurança utilizado.

Para outra corrente, a desatualização de *software* importa em um dispositivo vulnerável, logo se equivalendo a um dispositivo sem mecanismo de segurança. Um exemplo seria o agente que insiste em usar um sistema operacional antigo, com falhas facilmente exploráveis publicadas há anos (muitas delas exploráveis via *frameworks* como Metasploit), colocando-se em situação de risco diante de ataques cibernéticos. Outro exemplo seria o uso de servidor *FTP* com acesso de escrita, sistema de *upload* sem os filtros necessários, permitindo que o agente envie código malicioso para o servidor, dentre outros.

A questão é polêmica. Em nossa ótica, a perícia deverá ser sempre ouvida pelo juiz criminal a respeito da "atualização do sistema do dispositivo invadido", e como tal "desatualização" influenciava em uma invasão, quesitando ainda se tal "desatualização" tornava o sistema "literalmente aberto" a qualquer pessoa ou somente um especialista poderia explorar a desatualização, o que caracterizaria, via de regra, um "rompimento de obstáculo".

Outras questões que precisarão ser enfrentadas pela Justiça estão relacionadas com o caso do fabricante já disponibilizar a correção para uma falha antiga em seu sistema. A falha é pública e já tinha correção e não foi aplicada pela vítima do crime digital. Outro ponto polêmico será o caso de uma vítima com sistemas ou *softwares* piratas, que é invadida, e sua legitimidade ou não de acionar a Justiça para buscar a punição do invasor.

9.13.6. Sensitive Data Exposure

É sabido que muitas aplicações não protegem adequadamente dados pessoais, como número de cartões de crédito e outras credenciais de autenticação. Se o agente se apodera destas informações, sem esforço ou rompimento de obstáculo, não há que se falar em conduta criminosa. Ao se apoderar das credenciais, poderá acessar outros ativos e dispositivos, ainda assim não praticando crime algum, não "invadindo" dispositivo alheio. Importa dizer que da invasão condutas criminosas poderão advir, o que deverá ser apurado por perícia técnica.

9.13.7. Missing Function Level Access Control

Esta falha está relacionada à falta de controle de privilégio de usuários. O sistema deve permitir que o usuário somente acesse as páginas da aplicação que ele está autorizado a ver. Por exemplo, consideremos um sistema *web* voltado para publicação de notas. O correto seria o aluno somente conseguir consultar suas notas. Contudo, se ele conseguir acessar notas de outros alunos ou mesmo acessar áreas administrativas da sessão, estamos diante de uma falha grave. Em um simples exemplo, temos:

a) *Site*: www.escola.com.br

b) Aluno então acessa o sistema: www.escola.com.br/joao

c) Aluno simplesmente vai na URL (endereço do *site*) e troca o nome dele por outro e consegue acessar a página de uma segunda pessoa: www.escola.com.br/maria

d) Aluno simplesmente vai na URL e troca o nome dele pelo administrador, conseguindo acessar a página administrativa: www.escola.com.br/admin.

Não necessariamente, a falha pode ocorrer com alguém que esteja conectado no sistema. Por exemplo, alguém que nem estude nessa escola simplesmente pode acessar o endereço www.escola.com.br/admin e conseguirá ver a interface administrativa (explorando uma vulnerabilidade muito comum e uma padronização realizada por desenvolvedores de *sites* que mantém no diretório /admin o acesso administrativo ao sistema).

Deve-se destacar que, no exemplo, não se quebrou a senha de alguém, não se injetou código malicioso ou não se conseguiu passar código/parâmetros da URL do *site*. O que revela que páginas internas da aplicação *web* estão disponíveis para qualquer pessoa sem a devida autenticação ou filtro de acesso, podendo, inclusive, ser indexadas pelo Google ou outros buscadores. Para evitar essa brecha, normalmente são realizadas configurações de segurança nos servidores *web*, controle de autenticação no código da própria aplicação, checagem de privilégio do usuário sempre que acessar uma página ou *script* novo ou definição de outro processo que deve controlar os acessos às sessões administrativas da aplicação.

Por não haver, via de regra, violação de mecanismo de segurança, mas negligência dos próprios desenvolvedores, não há que se falar em aplicação do delito previsto no art. 154-A do Código Penal.

Do mesmo modo, o uso de aplicações como dirBuster e Acunetix, em que é possível testar vários nomes de arquivos diferentes para saber se se encontra algum acessível, em tese não seria conduta criminosa[91].

9.13.8. Cross-Site Request Forgery (CSRF)

Nesta falha, o atacante pode forçar o navegador ou aplicação vulnerável da vítima a gerar requisições *web* para obter dados e informações que seriam legítimas a esta, que está loggada (*logged-on*) no serviço ou dispositivo.

Percebe-se que, nesta manipulação, o agente não invade diretamente a vítima, mas dispara códigos a manipular o navegador desta, conduzindo ou fazendo com que ela mesma, que está loggada em um sistema, logo acessando legitimamente um dispositivo informático, realize requisições de dados ou informações a tais sistemas.

É como se o agente, impedido de entrar em um prédio, motivasse uma vítima, moradora, a entrar e trazer algum bem para ele. O problema é que no caso digital a vítima desconhece que está sendo utilizada. Por não haver "violação de mecanismo de segurança", em tese, não haveria de se cogitar da incidência do art. 154-A do Código Penal, no termos da Lei n. 12.737/2012 (embora existam entendimentos contrários).

Porém, se para explorar a vulnerabilidade aqui descrita o agente invadiu a vítima (conduta antecessora), passa a incidir o tipo em estudo (art. 154-A do Código Penal).

9.13.9. **Using Componentes with know Vulnerabilities**

Muitos componentes e dispositivos informáticos vulneráveis podem permitir o acesso com privilégio total, o que, se explorado, pode permitir ao atacante o acesso a dados e a indisponibilização do servidor, serviço ou dispositivo. A questão envolve a não implementação de *patches* de segurança pelos titulares dos ativos informáticos.

Uma situação é a vítima que está vulnerável a uma falha *0 day*, em que nem o fabricante tem a correção pronta ainda. Ela deve estar protegida pelo art. 154-A do Código Penal. Outra situação é a da vítima que, ciente da vulnerabilidade de um ativo, nada faz, assumindo o risco de usá-lo. É importante ressaltar que a Lei n. 12.737 não exige um "mecanismo de segurança atual", bastando qualquer forma de proteção. Por outro lado, como já salientado, é de bom tom que o magistrado ouça a perícia técnica, sempre que a questão envolver dispositivos com sistemas desatualizados ou componentes com conhecida vulnerabilidade.

9.13.10. Unvalidated Redirects and Forwards

Estamos diante do caso de aplicações que comumente redirecionam ou encaminham usuários para outras páginas e *websites*. Quando se utiliza de dados não validados para esta transmissão, permite que redirecione as vítimas para páginas falsas, de *phishing* ou *malware*, ou até mesmo use os encaminhamentos para acessar páginas não autorizadas.

Se o redirecionamento é feito para páginas falsas, não se pode falar em invasão de dispositivo informático. Se a vítima for lesada, pode-se cogitar do delito de estelionato (art. 171 do Código Penal) ou do furto mediante fraude (art. 155, § 4º, do Código Penal).

Se a falha é explorada e permite que o atacante acesse páginas não autorizadas, pode-se, mediante análise pericial, concluir pela invasão, considerando que a manipulação do *redirect* ou *forward* violou mecanismo de segurança da página, fazendo com que o *cracker* acessasse conteúdo privativo, logo, "obtendo informação".

9.14. A invasão de arquivos lógicos ou conteúdos protegidos em discos virtuais

Temos que um sistema informático pode ser conceituado como qualquer aplicação capaz de processar, capturar, armazenar ou transmitir dados, eletrônica ou digitalmente, ou de forma equivalente.

Já dispositivo de comunicação refere-se a qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia.

Por sua vez, a Convenção de Budapeste conceitua sistema computacional ou "sistema de computador" como qualquer dispositivo isolado ou um grupo de dispositivos relacionados ou interligados, em que um ou mais dentre eles desenvolve, em execução de um programa, o tratamento automatizado dos dados[92].

O art. 154-A do Código Penal não aproveita nenhum desses conceitos acima trazidos, dispondo

sobre a invasão de "dispositivo informático" sem conceituar tal expressão, o que pode gerar ampla e até prejudicial interpretação. Para alguns, dispositivo seria somente algo físico, *hardware*, capaz de armazenar ou até processar informações. Para outra corrente, dispositivo poderia ser um sistema informático ou um "ativo cibernético" protegido.

A legislação, como é sabido, exige que o dispositivo esteja protegido por mecanismo de segurança. O mecanismo pode ser uma mera senha, ou mesmo uma criptografia de disco, por exemplo, impedindo o acesso à informação (ou embaralhando o contexto informacional).

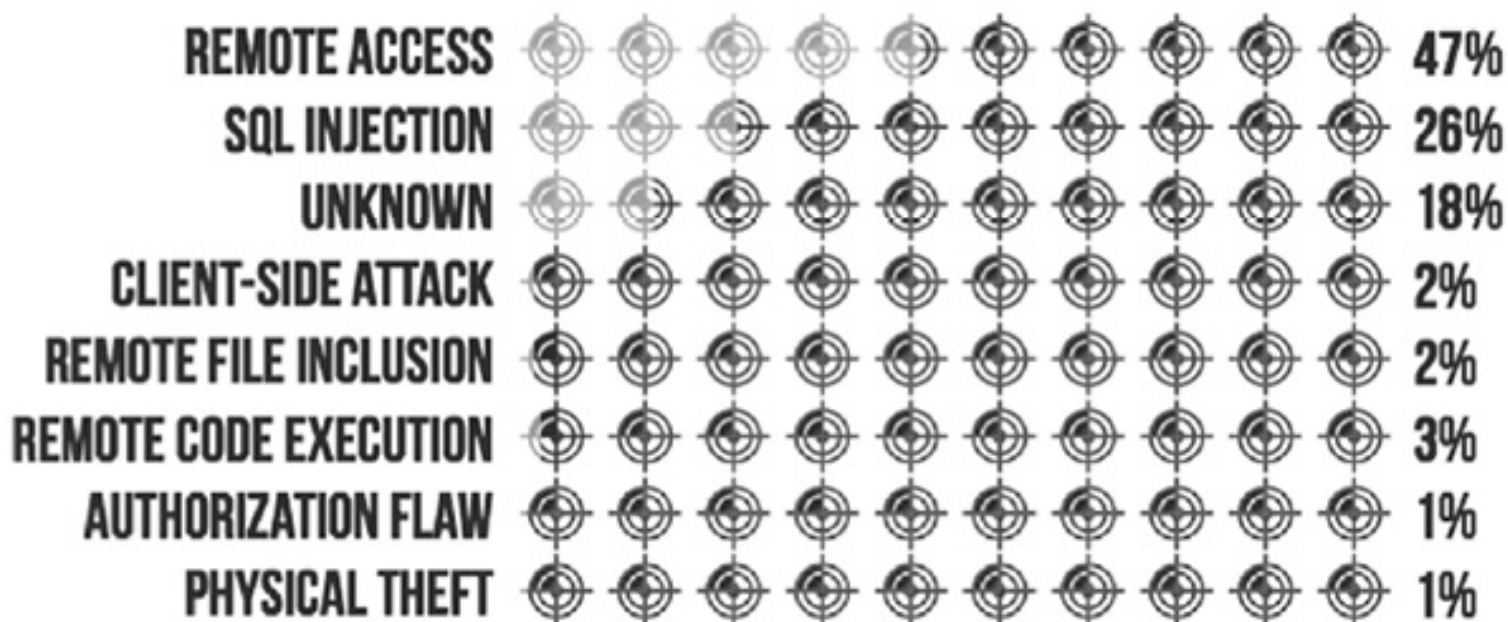
Da mesma forma que temos mecanismo de segurança (como a criptografia) aplicado a um telefone celular ou computador, também podemos, por exemplo, gravar informações em um "arquivo de lote" ou disco virtual, protegido por senha. Podemos, por exemplo, compactar várias informações em um arquivo (.zip) e protegê-lo por senha, ou mesmo esteganografar informações, que serão ocultadas em um arquivo base (*host*), que ficam protegidas por uma senha.

Em tal cenário, um agente que acessasse um computador desprotegido, mas lá quebrasse senha de um *software*, arquivo de lote, pasta protegida, ou disco virtual, acessando dados protegidos, poderia responder pelo delito do art. 154-A, recém-trazido pela Lei n. 12.737/2012?

A questão é polêmica e deverá passar pelas primeiras interpretações dos tribunais brasileiros. Em nossa ótica, tais recursos lógicos, protegidos por senhas, não se enquadram, em tese, no conceito de "dispositivo informático", pois na ausência de uma definição legal, não se pode estender o conceito para prejudicar um acusado. Deste modo, não haveria incidência do tipo envolvendo invasão de dispositivo informático para as questões contendo arquivos ou ativos virtuais com mecanismo de segurança.

9.15. O acesso remoto como método de invasão

A empresa de segurança da informação TrustWave lançou, em 2013[93], o documento chamado "Global Security Report", relatório completo sobre ameaças a ciber-segurança no mundo.

Dentre os oito principais métodos de entrada em um ativo informático alheio, encontramos, com 47%, o *Remote Access*, seguido da invasão pela técnica *SQL Injection*:

Percebe-se que, segundo a empresa, grande parte das invasões computacionais decorre do acesso remoto a outros dispositivos. Mas, como ficará o acesso remoto no âmbito da Lei n. 12.737/2012?

Um dispositivo pode estar com o sinal “Bluetooth” ativado, deixando o equipamento descoberto, podendo ser acessado por qualquer usuário. Se, para o acesso não existia senha para o “emparelhamento”, não há que falar em invasão de dispositivo informático. A vítima se colocou em situação de risco e excluiu a incidência da Lei n. 12.737 ao não adotar segurança em seus ativos.

Hoje, grande parte dos dispositivos permite o acesso remoto. É dever do usuário bloquear o acesso ou inserir no mínimo uma palavra-passe para que terceiros não autorizados não procedam com o precitado acesso. Neste sentido, a vítima que mantém dispositivo com possibilidade de recebimento de conexões remotas, sem senha, assume o risco da conduta omissiva ou comissiva e, se tiver dispositivo invadido, não contará com o apoio da Lei n. 12.737.

Neste sentido, Milagre (2013, p. 1) salienta que “outras formas de acesso indevido, onde não ocorre a ‘invasão’, que é conduta comissiva/ativa, podem não se enquadrar no tipo penal. Assim, na

engenharia social que faz com que a vítima forneça credenciais de acesso ou mesmo acesse voluntariamente determinado programa que libera o acesso a seu dispositivo, fica eliminada, em tese, a incidência do delito em comento, podendo o agente, diante do caso concreto, responder por outros delitos do Código Penal, de acordo com a extensão do dano. Do mesmo modo, o acesso indevido feito por um agente através de protocolo RDP (Remote Desktop Protocol) ou tecnologias como Terminal Service, VNC, PCAnywhere, Logmein, dentre outras, não caracterizam invasão se o serviço de 'assistência remota' foi habilitado pelo titular do dispositivo sem qualquer mecanismo de autenticação, o que equivaleria a uma 'autorização tácita' do titular do dispositivo para acessos".

Tomemos outro exemplo para reflexão relacionado à vulnerabilidade *Heartbleed*.

A *Heartbleed* é uma vulnerabilidade ou falha que explora o serviço de comunicação segura em rede SSL (*Secure Sockets Layer*), diga-se, um mecanismo de segurança para as comunicações. A vítima, ao usar um serviço SSL vulnerável, permite que alguém acesse os dados da memória do seu equipamento, em texto plano. Logicamente, o atacante, para obter tais informações, deverá se valer de um programa *exploit* (código usado para explorar vulnerabilidade). O *exploit*, então, simplesmente reconhece a vulnerabilidade e realiza a cópia *dump* das informações. Neste cenário, dois entendimentos surgem:

O primeiro entendimento enaltece que no caso ocorre um acesso indevido às informações, mas não propriamente dita uma "invasão", considerando que, a princípio, não existe rompimento de obstáculo, barreira tecnológica ou violação de mecanismo de segurança. O serviço da vítima já não tinha mecanismo de segurança ao estar vulnerável pela *Heartbleed*. O que o atacante faz, então, é simplesmente acessar indevidamente o que estava "aberto" e coletar as informações. Não haveria o crime do art. 154-A do Código Penal.

Já o segundo entendimento registra que, em que pese o sistema de a vítima estar vulnerável à *Heartbleed*, não seria qualquer pessoa que teria o acesso aos dados, de forma simples e trivial, mas somente aquelas que usaram o *exploit* (e souberam como usá-lo) e, neste sentido, o *exploit* é que

explora/interage com a vulnerabilidade e rompe os obstáculos e barreiras, realizando a violação de mecanismo de segurança, permitindo o acesso a dados de modo não convencional. Haveria o crime do art. 154-A do Código Penal.

Em outro exemplo, a vítima que instala roteador Wi-Fi (rádio) sem senha[94], ou mesmo utiliza a senha padrão do fabricante (muitas vezes impressa no próprio equipamento ou etiquetada neste), que recomenda sempre a imediata alteração. Neste caso, igualmente, não houve rompimento de obstáculo nem violação de mecanismo de segurança, não havendo de se cogitar do crime previsto no art. 154-A do Código Penal.

9.16. O *reversing* e a publicação das falhas encontradas e provas de conceito

Deve-se destacar que a lei não faz distinção entre *software* livre ou proprietário invadido. Não importa se o *software* é livre ou proprietário (no livre só vai ser mais fácil ver a fonte para detectar a falha explorada). Já no caso do *software* proprietário, se o agente executa o *reversing* (engenharia reversa) em código compilado em um *firmware* de um roteador, por exemplo, e lá identificar falha ou consegue alterar o código para fazer o binário se comportar de modo inesperado, tem-se o crime de violação autoral, plágio, previsto no art. 184 do Código Penal, considerando que, nos termos da Lei n. 9.610/98, cabe ao autor o direito de autorizar qualquer modalidade de uso de sua obra, também incidindo o art. 12 da Lei n. 9.609/98 ("Lei do Software").

Questão polêmica diz respeito à publicação de *exploits*, aptos a explorarem uma falha identificada em um ou vários sistemas. Nos termos do § 1º do art. 154-A do Código Penal, na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

Assim, aquele que difunde "código" para exploração de uma falha só poderá ser responsabilizado, em nossa ótica, se o código efetivamente proporcionar a "invasão de dispositivo informático protegido por mecanismo de segurança com os fins previstos em lei". Então, nem toda a divulgação

de *exploit* pode ser considerada ilegal. Por outro lado, a lei silencia em relação àquele que divulga "guia", "orientação", "notícia" ou "manual para exploração de determinada falha". Neste caso, o agente não divulga o explorador, mas explica, na teoria, como deve ser feita a exploração. Logo, tal conduta é atípica. Um exemplo é um pesquisador que divulga em seu *blog* como se faz para explorar ou invadir dispositivo com sistema operacional Windows 7. Ou o agente que faz um *paper* para um congresso demonstrando como se viola determinado sistema. Esta demonstração deve ser impessoal, teórica, sem referenciar determinada vítima ou expor dados pessoais.

Igualmente, a divulgação da "prova de conceito", que demonstra a exploração de uma vulnerabilidade, em tese não é criminosa, mas não deixa de ser uma prova apta a demonstrar que o agente (ou alguém) cometeu uma anterior "invasão". É preciso cautela. Neste cenário, a prova de conceito deve ser genérica, resumida, impessoal e não mencionando caso específico (quando possível), nem retornando dados pessoais, limitando-se a demonstrar a falha minimamente impactando na violação de dados ou imagem corporativa. Embora, em segurança da informação, prova de conceito seja o desenvolvimento de uma ferramenta prática para provar a vulnerabilidade teórica de um sistema de informação, tal ferramenta pode ser feita de modo a "não permitir a exploração por terceiros", o que afasta a incidência criminosa.

As pesquisas de segurança não podem ser consideradas criminosas, ainda que sem conhecimento dos titulares dos ativos. É possível realizar as pesquisas sem necessariamente invadir. Diga-se, demonstrar em *paper* artigo, postagem ou prova de conceito, a insegurança de um sistema, sem lesar usuários ou expor seus dados, ou mesmo sem consumar uma invasão. Um exemplo, no *framework* Mestasploit, é um caso em que podemos verificar um *host* vulnerável a uma falha (escanear o *host*), sem chegar a executar o *exploit*, em que teria se iniciado a execução da invasão. Outro exemplo, no *software* sqlmap (que permite *sql injection*), em que podemos avaliar um banco de dados vulnerável sem listar as tabelas. Serão práticas que os profissionais de segurança precisarão desenvolver e assimilar. A linha é tênue e é preciso ficar atento ao entendimento jurisdicional, que pode mudar.

Neste contexto, em que pese a prova de conceito, para alguns pesquisadores, necessariamente ter que apresentar o *exploit*, o que vai diferir para fins da conduta criminosa, o que é decisivo em muitas situações (para provar ou não a intenção do agente), será o *payload* ou o que está sendo passado ao sistema testado. Um exemplo seria, após a invasão ou o agente conseguir *ownar* o sistema (tomar conta do sistema), o agente em vez de carregar um *payload* para tomar a *shell*, obter ou manipular os dados, usa um *payload* para abrir a calculadora. Invadiu, usou ferramenta que permite a invasão, mas não praticou crime, pois restou claro que sua "intenção" não era obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidades para obter vantagem ilícita. No que tange a disponibilizar a ferramenta, da simples análise do código, será possível concluir que, embora esteja sendo divulgada, percebe-se que não visa invasão com a finalidade prevista em lei (obter, adulterar dados ou instalar vulnerabilidades).

Por fim, é preciso esclarecer que pesquisas feitas em laboratórios, ou ambientes controlados, não constituem, ainda que haja invasão a dispositivos, conduta criminosa, considerando que os ativos são dos próprios pesquisadores ou, quando não, estes possuem autorização para exploração, firmada pelos proprietários.

9.17. *Malware as a service* e ataques de negação de serviços encomendados

Uma nova tendência do cibercrime é denominada *Malware as a service* ou mesmo *DDOS as a service*, técnicas nas quais o atacante pode encomendar um ataque contra um alvo específico.

A facilidade não deixa de ser um complicador forense, sobretudo quando um agente, situado no Brasil, contrata um serviço no exterior, para atacar uma vítima também em território nacional.

Em que pese saber que a competência para apuração de crimes desta natureza é da Justiça brasileira, a investigação é um complicador, considerando que as empresas que oferecem estes serviços comumente estão em paraísos eletrônicos, não tendo dever de cooperar com autoridades no fornecimento de dados dos autores ou mandantes do crime.

Nos termos da Lei portuguesa n. 109/2009, aqueles que disponibilizam serviços que permitem a invasão, ou destinados a produzir as ações não autorizadas, podem responder nos termos do item 2 do art. 6º. Vejamos:

Artigo 6º

Acesso ilegítimo

1 – Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3 – A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 – A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 – A tentativa é punível, salvo nos casos previstos no n. 2.

6 – Nos casos previstos nos ns. 1, 3 e 5, o procedimento penal depende de queixa.

No Brasil, existe disposição similar no § 1º do art. 154-A do Código Penal. Deste modo, pelo delito será responsabilizado o executor do ataque, e, se identificado, também será responsabilizado seu mandante, contratante dos serviços.

Deve-se ponderar, no entanto, que o ataque de negação de serviços só será punível, no Brasil, se atentar contra serviços públicos ou de utilidade pública. Isto demonstra que as leis existentes são

ainda ineficazes, em muitos casos, para a proteção dos particulares. Para sistemas de particulares, a proteção poderá se dar, por analogia, pelo art. 163 do Código Penal, pelo que sabemos, é forçoso e ilegal.

9.18. Lei n. 12.737/2012 e a invasão com o objetivo de instalação de vulnerabilidades

Vulnerabilidade pode ser conceituada como a incapacidade de suportar os efeitos de um ambiente hostil. Dentre os tipos de vulnerabilidade, podemos citar a social, relacionada à incapacidade de indivíduos e organizações de resistirem a impactos adversos de fontes estressoras e de choque.

Incapacidade de suportar danos ou ataques é em síntese a vulnerabilidade. Na informática, é conceituada como a fraqueza que permite uma exploração. Está relacionada a três elementos: a suscetibilidade do sistema ou falha, o acesso do atacante a falha e a capacidade do atacante de explorar a falha.

O invasor, necessariamente, deve ter uma ferramenta ou técnica que possa se aplicar à fraqueza ou vulnerabilidade específica de um sistema. Um sistema pode estar vulnerável a um ataque e não a outro.

ISO 27005, IETF RFC 2828, NIST, ENISA, The Open Group, FAIR e ISACA são algumas normas e instituições que definem a vulnerabilidade. Todas as definições no mundo remetem à ideia da fraqueza de um ativo que pode ser explorada por uma ou mais ameaças.

Fraquezas essas que podem surgir na concepção, implantação, operação ou gestão de um sistema. Vulnerabilidade é ainda a probabilidade de um ativo não ser capaz de resistir às ações de uma ameaça. Vulnerabilidade é, *grosso modo*, qualquer fraqueza ou falha existente em um sistema.

A vulnerabilidade pode se dar em um *software*, em uma rede, ou mesmo em uma pessoa que sucumbe a um ataque de um *hacker*. Uma senha fraca, por exemplo, é uma vulnerabilidade. Um computador com senha forte pode estar vulnerável em outro ponto, a despeito da senha. Comumente,

um *bug* de *soft-ware* que pode ser explorado para o ataque é um exemplo de vulnerabilidade comum. Não resta dúvida de que o ponto mais vulnerável, na maioria dos sistemas de informação, é o elemento humano, vítima constante da engenharia social. O agente que obtém credenciais de acesso a um banco de dados protegido, valendo-se da interação com usuários, está explorando uma vulnerabilidade.

Um estado vulnerável é um estado autorizado, a partir do qual um estado não autorizado pode ser alcançado usando transições de estados autorizados. Logicamente, por definição, um ataque ou uma invasão começa necessariamente em um estado vulnerável. Quem invade, via de regra, invade algo vulnerável ou graças a uma vulnerabilidade relacionada ao objeto, e não é comum que invada para "instalar uma nova vulnerabilidade".

Pois bem, ignorando o que mencionamos, o art. 154-A do Código Penal, acrescentado pela Lei n. 12.737/2012, assim define o tipo de invasão de dispositivo informático:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, ***mediante violação indevida de mecanismo de segurança*** *e* ***com o fim de*** *obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo* ***ou instalar vulnerabilidades para obter vantagem ilícita****:*

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Ora, se alguém invade um dispositivo informático mediante violação indevida de mecanismo de segurança, de fato está explorando alguma vulnerabilidade relativa ao dispositivo, que tinha uma fraqueza direta ou em relação aos responsáveis pelo ativo. Deste modo, explorando a vulnerabilidade, violou o modo comum de acesso ao sistema ou o mecanismo de segurança e obteve acesso indevido ao sistema. Estando no sistema, o agente pode obter, adulterar ou destruir dados e informações ou mesmo instalar códigos para prejudicar ou lesar a vítima. Não faz sentido o que um atacante invada, explorando necessariamente uma vulnerabilidade com o objetivo de instalar outra vulnerabilidade!

A sugestão para a redação do artigo citado seria: *Invadir dispositivo informático alheio, conectado ou não à rede de computadores,* ***mediante violação indevida de mecanismo de segurança*** *e* ***com o fim de*** *obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo* ***ou instalar código ou sistema para obter vantagem ilícita***.

A vulnerabilidade é ativada por uma ameaça, a vulnerabilidade é explorada, e pode atentar contra a integridade, a confidencialidade e a disponibilidade da informação.

Como foi possível constatar, a vulnerabilidade é uma fraqueza em um sistema. Não se espera de um atacante, que acaba de invadir um sistema, que "instale uma vulnerabilidade". Ele vai tirar proveito! No máximo, a vítima pode instalar um sistema vulnerável, que poderá ser explorado pelo atacante. Falar em instalar vulnerabilidade, como objetivo da invasão, para um *cracker*, seria o mesmo que dizer ao atacante para criar uma nova porta em um quarto no qual ele já entrou, ou mesmo que punir um ladrão de veículos que, ao arrombar a porta do carro, em vez de levar o bem, abre todas as demais portas e vai embora.

A situação da redação é grave, pois estamos lidando com a liberdade de indivíduos, com o Direito Penal e seu princípio da legalidade. Nosso escopo, com o livro, é no mínimo mostrar que legislar sobre informática pode ser mais difícil do que parece. Mais que isso, interpretar leis de informática ou Internet é ainda mais dificultoso. Neste cenário, o agente que invade um sistema informático não obtém, não adultera nem destrói informações, mas simplesmente instala aplicação ou código malicioso para capturar dados bancários da vítima; como se verifica, não invadiu com o fim de "instalar vulnerabilidade", mas com o fim de "explorar vulnerabilidade" já existente, instalando código malicioso. Logo, não poderá ser punido pelo art. 154-A do Código Penal.

Este é resultado de legislar por casuísmos. Uma lei para fazer frente ao crime digital, que já nasce com certa carga de ineficácia e repleta de deficiências.

9.19. O que pode ser considerado mecanismo de segurança

Como vimos, é indispensável que o ativo a ser invadido esteja protegido por mecanismo de segurança ou barreira tecnológica. Em segurança da informação, mecanismos de segurança podem ser considerados "proteções" ou medidas que objetivam livrar a informação de situações que possam causar danos.

As proteções são lógicas, como permissões em sistemas de arquivos, *fire-walls* ou senhas, e sistemas de detecção de intrusos, físicas, como cofres, portas, fechaduras, e administrativas, como políticas, normas e procedimentos.

Para fins do disposto no art. 154-A acrescentado pela Lei n. 12.737/2012, que tipo de mecanismo de segurança deve ser evidenciado? Lógico, físico ou administrativo?

É uníssono o entendimento de que a proteção lógica é a mais comum. Existem entendimentos de que a proteção física também pode caracterizar "mecanismo de segurança" descrito no crime de invasão, como, por exemplo, no caso da vítima que guarda seu *pen drive* em um cofre ou sala fechada. Assim, em caso de arrombamento, estaria caracterizado o tipo comentado (Invasão de dispositivo informático – art. 154-A do Código Penal), considerando a existência de mecanismo de segurança físico (fora do dispositivo, mas que o protege). O entendimento não é pacífico.

Quanto às proteções administrativas, entendemos que elas não incorporam o conceito de "mecanismo de segurança" descrito no art. 154-A do Código Penal, mais se assemelhando a "ausência de autorização" para acesso a determinado dispositivo. Como exemplo, posso ter uma norma que proíbe colaboradores de determinada área de acessarem conteúdos de outro setor, mas caso um destes colaboradores acesse, não poderemos afirmar que houve violação de mecanismo de segurança, mas tão somente acesso não autorizado. Logo, não havendo violação de proteção, não haveria invasão e o fato seria atípico.

9.20. Conter uma invasão e se desproteger da lei

A Lei n. 12.737/2012 impacta em diversos domínios da disciplina da segurança da informação. Sempre que um delito ocorre, o time de resposta a incidentes, se o detecta em tempo real, é incumbido de conter o ataque imediatamente.

Ocorre que, de acordo com o estágio do ataque, não será possível apurar a intenção do agente. Imagine que o atacante inicia a invasão e imediatamente é interrompido pelo time de resposta a incidentes. Embora já estivesse dentro da máquina, não chegou a executar sua sequência de comandos, que demonstrariam sua real intenção.

Não sendo demonstrada a intenção, o dolo (elemento subjetivo do tipo), como punir o agente? Em determinados casos, talvez, seja necessário que a equipe de segurança “dê corda” ao agente, até ter dados suficientes para provar seu intento. Tal conduta envolve muita experiência, circunstâncias especiais e preparo técnico.

10.

LEI DE CRIMES INFORMÁTICOS E A INVESTIGAÇÃO CIBERNÉTICA

10.1. Marco Civil da Internet e a estrutura investigativa

A Lei n. 12.737/2012 longe está de solucionar todos os problemas relativos ao crime cibernético no Brasil. A solução não é fácil de ser encontrada, mas com certeza não resolve tão somente com a edição de leis e mais leis criminais. Envolve educação digital, políticas criminais e estrutura investigativa.

O Marco Civil da Internet é considerado a "Constituição da Internet", garantindo direitos e deveres a todos os atores da Internet brasileira (usuários, provedores de conexão e de serviços em geral). Fruto de um projeto nascido em 29 de outubro de 2009, da Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, o Marco Civil foi uma construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010, tendo recebido mais de duas mil contribuições[95].

Após a fase de participação popular, ingressou no Congresso em 24 de agosto de 2011, por meio do Projeto de Lei n. 2.126, de iniciativa do Poder Executivo, projeto que visou estabelecer princípios, garantias, direitos e deveres para o usuário da Internet no Brasil[96]. A legislação tem escopo de evitar, igualmente, decisões contraditórias proferidas pelo Judiciário, em casos semelhantes envolvendo tecnologia da informação, gerando insegurança jurídica.

Foi sancionado pela Presidência da República em 23 de abril de 2014, tornando-se a Lei n. 12.965. Cogita-se, ainda, da propositura na Assembleia das Nações Unidas de um possível Marco Civil Internacional. O Marco Civil da Internet pode ser integrado às leis objeto de estudo neste livro.

São complementares nas atividades envolvendo repressão a crimes cibernéticos.

O Marco Civil é considerado uma vitória da sociedade brasileira. Uma reclamação da sociedade civil, em 2009, que repudiou as iniciativas no sentido de criminalizar condutas na Internet, exigindo, antes, que o Congresso desse uma carta de direitos dos internautas.

A Lei n. 12.737/2012, como visto, tipifica fatos cibernéticos, porém não trata de estrutura investigativa ou deveres dos provedores de Internet e serviços no que tange à cooperação para com autoridades na investigação de crimes digitais. A Lei n. 12.735/2012 (Lei Azeredo), por sua vez, chega a prever que os órgãos de polícia judiciária poderão estruturar, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em redes de computadores, dispositivo de comunicação ou sistema informatizado.

Neste raciocínio, sabe-se que, no Brasil, ninguém é obrigado a fazer ou deixar de fazer algo, senão em virtude de lei (princípio da legalidade). Neste sentido, até o advento do Marco Civil, no Brasil, inexistia lei que obrigasse os provedores de Internet ou de serviços a registrarem *logs* das atividades de seus usuários.

Por outro lado, existia apenas "recomendação"[97] do Comitê Gestor Internet do Brasil, para que os provedores (de acesso) passassem a manter, por prazo mínimo de 3 (três) anos, dados de conexão e de comunicação realizadas por seus equipamentos (identificação do endereço IP, data e hora de início e término da conexão e origem da chamada), o que refletia também o posicionamento do Superior Tribunal de Justiça.

Sabe-se que na grande maioria dos crimes digitais, em que a vítima não é administradora do ativo informático utilizado para a prática do crime ou do ativo atacado, para que se apure a autoria do delito, faz-se indispensável a cooperação de terceiros, que geralmente administram e oferecem os serviços, aplicações ou *hosts* utilizados para a prática dos delitos ou que serviram de ambiente para o crime digital.

Dentre esses terceiros, os mais solicitados são os provedores de serviços de Internet (aplicações)

e os provedores de conexão à Internet. Inicialmente, pela ordem, busca-se um contato com aqueles, e, posteriormente, com estes.

Quando alguém se conecta na Internet, para boas ou más finalidades, o faz através de um ISP (*Internet Service Provider*), ou provedor de acesso à Internet. Este provedor atribui ao usuário um endereço IP (*Internet Protocol*), em uma determinada faixa de data e horário – comumente enquanto durar a conexão à Internet. Tal atribuição pode ficar registrada no provedor de conexão (registros de conexão associados a dados cadastrais). O usuário, por sua vez, ao interagir com serviços na Internet (hospedagem, *blogs*, *e-mails*, *chats*, discos virtuais, redes sociais, mensageiros, serviços de vídeos etc.), tem seus dados registrados por estas aplicações, o que se chama de "registro de acesso a aplicações na Internet", que contém várias informações sobre o uso do serviço *web* por tal usuário (data, hora, IP, fuso horário associado ao uso de determinada aplicação).

Deste modo, diante do uso criminoso de um serviço, ainda que de forma anônima, como, por exemplo, na criação de uma comunidade, grupo, ou página destinada à pornografia infantil, sabe-se que o provedor dos serviços (pago ou gratuito) registra os dados de acesso à aplicação (em alguns casos, até mesmo as atividades realizadas – embora muitos afirmem que não), porém tais registros só são fornecidos com ordem judicial. Obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP (*Internet Protocol*), que será fornecido, descobrir qual o Provedor de Acesso associado ao IP (caso o usuário não tenha mascarado a conexão), e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa[98].

Por meio desta correlação, pode-se chegar à autoria de delitos cometidos por meio da Internet, comumente praticado por pessoas que "não se identificam nos serviços" para criação ou acesso aos mesmos, utilizados para práticas criminosas. Logicamente, pode ocorrer de o titular de uma conta de Internet não ser o agente criminoso; neste caso, pode responder por ter negligenciado, permitindo que

terceiros acessassem seus ativos, como, por exemplo, no caso de usuário que deixa Internet a rádio, *wireless*, de sua residência, desprotegida, permitindo que terceiros acessem e pratiquem crimes por meio de sua conexão. Titulares de Lan Houses (cibercafés), por exemplo, devem guardar dados em determinados estados por até 60 (sessenta) meses[99].

Neste contexto, como fica evidenciado, sem a cooperação dos provedores de Internet ou de serviços, em muitos casos, é praticamente impossível apurar a autoria de delitos cibernéticos, e a questão se agrava quando um destes provedores não está no Brasil. A Lei n. 12.737/2012 não trata a este respeito, logo, ao trazer tipos penais, sem fornecer estrutura investigativa, não coopera efetivamente para a redução dos crimes cibernéticos.

Já o Marco Civil da Internet traz disposições que interessam ao tema investigação. Embora não seja objeto deste livro[100], teceremos algumas considerações sobre a Lei n. 12.965/2014, por guardar relação também com crimes cibernéticos e formas de investigação.

10.1.1. Inviolabilidade do sigilo às comunicações na Internet

Nos termos do inciso I do art. 7º do Marco Civil, os usuários passam a ter direito à inviolabilidade e ao sigilo de suas comunicações na Internet, exceto por ordem judicial, para fins de investigação criminal ou instrução processual penal.

Fica extinta a possibilidade de grampos informáticos concedidos na esfera cível, o que atualmente ocorre em processos envolvendo concorrência desleal, fraude, dentre outros.

Nos moldes do inciso V do precitado artigo, o usuário tem direito ao não fornecimento a terceiros de seus registros de conexão e de acesso a aplicações na Internet, salvo mediante consentimento ou nas hipóteses previstas em lei.

10.1.2. Guarda de **logs** *de acesso à Internet e aplicações*

O Marco Civil consigna em lei que somente por ordem "judicial" os provedores serão obrigados a

disponibilizar os registros e informações que permitam a identificação de algum usuário. Do mesmo modo, a remoção de conteúdos só será cabível diante de um mandado, com exceção dos casos envolvendo fotos de nudez, em que a mera notificação extrajudicial deverá ser atendida pelos provedores de conteúdo, vejamos:

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput *deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.*

No que diz respeito à guarda de registros de conexão pelos provedores de acesso (que simplesmente conectam o usuário na Internet), o Marco estabelece, em seu art. 13, que os provedores têm o dever de manter os registros pelo prazo de 1 (um) ano.

Já os provedores de aplicações ou serviços de Internet (que oferecem serviços ou utilidades na Internet), nos termos do art. 15, deverão guardar os registros de acesso a aplicações por 6 (seis) meses. Importa dizer que o fornecimento dos registros somente poderá se dar por ordem judicial, sendo que autoridades administrativas, como Polícia e Ministério Público, poderão requerer aos provedores a guarda por mais tempo do que o previsto em lei, obrigando-se, no entanto, a ingressarem com o requerimento judicial dos dados.

10.1.3. A quebra de sigilo, o Ministério Público, autoridade policial e a Lei n. 12.683/2012

O Marco Civil não trata de interceptação telemática. Pelo contrário, proíbe claramente a

interceptação das comunicações de usuários de Internet (exceto para fins de investigação criminal), prevendo somente a hipótese da guarda de *logs*, em determinados casos, que serão fornecidos mediante ordem judicial de “quebra de sigilo”.

Importa dizer que quebra de sigilo envolve dados armazenados, que não estão “em comunicação”. Logo, não há de se cogitar em “proteção das comunicações”. Nesse sentido:

“(…) IV – Proteção constitucional ao sigilo das comunicações de dados – art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, *DJU* 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada – o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa – este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve ‘quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial’. 4. A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação ‘de dados’ e não dos ‘dados em si mesmos’, ainda quando armazenados em computador (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira – *RTJ* 179/225, 270). V – Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º, e 114, II; e Súmula 497 do Supremo Tribunal)”.

Com efeito, embora seja ponto polêmico, permanece afastada a possibilidade de agentes do Ministério Público requererem diretamente aos provedores os registros desejados (de conexão ou

acesso a aplicações).

Neste sentido, também dispõe a Lei Complementar n. 75, de 20 de maio de 1993, que prevê as atribuições do Ministério Público da União:

Art. 6º Compete ao Ministério Público da União:

(...)

XVIII – representar;

a*) ao órgão judicial competente para quebra de sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, para fins de investigação criminal ou instrução processual penal, bem como manifestar-se sobre representação a ele dirigida para os mesmos fins;*

(...)

No que diz respeito à possibilidade de a autoridade policial (delegados de polícia) requerer diretamente dados aos provedores, em que pese ser uma antiga reivindicação das autoridades (muitas, propostas na fase inicial do Marco), o Marco Civil é claro ao prever que o fornecimento de dados envolvendo registros de conexão ou de acesso a aplicações só é autorizado mediante ordem de um Juiz de Direito (autoridade judiciária).

De ver-se, no entanto, que, no âmbito dos crimes de lavagem de dinheiro, em 9 de julho de 2012 foi aprovada a Lei n. 12.683 para tornar mais eficiente a persecução penal dos crimes desta natureza, previstos na Lei n. 9.613, de 3 de março de 1988. Deste modo, passa a dispor a lei comentada:

Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

Neste cenário, especificamente no que concerne aos delitos de lavagem de dinheiro, já existe a

possibilidade de a Polícia e o Ministério Público acessarem determinados dados, sem a necessidade de ordem judicial.

Reforçando o disposto acima, o Marco Civil autorizou autoridades policiais e Ministério Público ao acesso de dados cadastrais de usuários, mediante simples requerimento. Vejamos:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

(...)

§ 3º O disposto no caput *não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*

No entanto, não se deve confundir dados cadastrais com dados de conexão ou acesso a aplicações. Enquanto aqueles podem ser obtidos via requerimento direto aos provedores, estes somente via ordem judicial.

O Marco Civil prevê que a autoridade policial, administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de Internet ou de conexão, que os registros de acesso a aplicação ou de conexão sejam guardados por prazo superior ao legal (art. 15, § 2º, e art. 13, § 2º). Em qualquer das hipóteses, o fornecimento dos dados só poderá ocorrer com autorização judicial.

Ademais, já tramita no Senado o Projeto de Lei n. 180/2014[101], que pretende estabelecer modificações no funcionamento do Marco Civil, sendo que uma das alterações é que o requerimento de autoridade policial ou do Ministério Público para a guarda de registros por mais tempo se dê, igualmente, mediante ordem judicial.

Como explica Milagre (2014, p. 1), “em relação ao requerimento de guarda de dados por mais

tempo do que o legal, a ser feito pelo Delegado ou Ministério Público, a lei complica a vida destas autoridades, exigindo que tal requerimento seja judicial".

10.1.4. Responsabilidade do provedor de aplicações

Nos moldes do art. 18 da Lei n. 12.965/2014, tem-se que o provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Importante mencionar que, nos termos do art. 19 do Marco Civil, o provedor de aplicações de Internet pode vir a ser considerado responsável por atos de terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente. O artigo, no entanto, consigna: *ressalvadas as disposições legais em contrário*.

Deste modo, poderá haver hipóteses legais em que o provedor de aplicações de Internet possa vir a ser responsabilizado por conteúdo de terceiros, mesmo diante da ausência de ordem judicial específica para remoção de conteúdos infringentes ou violadores.

Atualmente, temos decisões divergentes a respeito, sendo que, em muitos casos, provedores eram condenados por não atenderem notificação extrajudicial da vítima para remoção de determinado conteúdo da Internet. O Marco Civil vem trazer um parâmetro (ainda que mínimo), evitando decisões contraditórias.

Não existe óbice, por fim, para eventual responsabilização criminal de diretores ou sócios de provedores de acesso ou de aplicações, desde que comprovada participação ou coautoria em crime informático ou crime cometido por intermédio da informática.

10.2. Interceptação telemática e a Lei n. 9.296/96

As novas leis de crimes cibernéticos não tratam da interceptação telemática (tampouco a criminaliza), instrumento muitas vezes útil à investigação de delitos cibernéticos. Tal disposição já

se encontra prevista na Lei n. 9.296/96[102], que dispõe: *A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça*.

Deve-se esclarecer que a interceptação deve ser negada sempre que a prova puder ser realizada por outros meios. Não obstante, não será admitida a interceptação nos fatos investigados nos quais para a infração seja cominada pena de detenção.

Sobre a proibição de interceptação autorizada para crimes apenados com detenção, importa dizer que o PL n. 84/99, em sua gênese, buscava remover tal restrição. Como cediço, tal dispositivo foi suprimido durante o trâmite no Congresso, não prevalecendo quando da convalidação em Lei n. 12.735/2012, razão pela qual permanecem válidas as disposições da Lei de interceptação telemática brasileira.

Muito se questiona se o Provedor de Telemática ou Telecom poderia se negar a conceder acesso ao sistema de interceptação para autoridade policial que se nega a fornecer cópia da decisão autorizadora (mandado). Neste sentido:

“PROCESSUAL PENAL. *HABEAS CORPUS* PREVENTIVO. QUEBRA DE SIGILO DE DADOS CADASTRAIS. ORDEM JUDICIAL. FORNECIMENTO DE SENHAS A POLICIAIS FEDERAIS. DESCUMPRIMENTO PELA OPERADORA DE TELEFONIA. ILEGALIDADE NÃO VERIFICADA. ORDEM DENEGADA.

I – *Habeas corpus* preventivo, no qual busca o paciente, gerente da área de quebra de sigilo da empresa de telefonia, assegurar que não lhe sobrevenha qualquer consequência penal em razão do descumprimento de ordem judicial que, por sua vez, determinou o fornecimento de senhas ao Delegado e Agentes da Polícia Federal que os habilitassem junto à operadora de telefonia a obter dados cadastrais de terminais telefônicos móveis celulares.

II – Verificou-se tratar de procedimentos restritos às pessoas dos investigados. De fato, o

magistrado *a quo*, cautelosamente, ressalvou que as consultas limitam-se ao interesse da investigação.

III – Observou-se, ainda, que a senha a ser conferida ao Delegado e Agentes da Polícia Federal tem prazo determinado de 15 (quinze) dias e deve ser utilizada exclusivamente no interesse da investigação. Assim, não há que se falar em senha genérica, uma vez que restou claro se tratar de senha pessoal e intransferível, sendo de inteira responsabilidade do seu usuário a utilização indevida da mesma.

IV – Inclusive, nos ofícios impugnados ficou consignado que a autoridade policial deverá comunicar ao juízo todas as consultas formuladas pela autoridade policial, medida que visa propiciar o controle judicial.

V – Outrossim, a autorização judicial ora questionada foi proferida em autos regularmente distribuídos e processados perante o juízo competente, estando sujeito ao controle do Ministério Público Federal e do Poder Judiciário, motivo pelo qual, eventual utilização indevida das senhas é passível de imediata reparação.

VI – O não encaminhamento de cópia da decisão que decretou a quebra do sigilo de dados à operadora de telefonia e ao paciente justificou-se, haja vista se estar diante de investigação que tramita em segredo de justiça, incumbindo às autoridades e servidores que atuem nos feitos zelar pelo sigilo da mesma, sob pena de frustrar-se a apuração dos fatos e colocar-se em risco a integridade física dos investigados.

VII – Ainda, não se restringem as medidas adotadas à competência territorial do juízo coator, pois a atividade criminosa não se limita a ela.

VIII – Embora compita à operadora de telefonia zelar pelo sigilo dos dados cadastrais de seus usuários (artigos 3º e 72 da Lei n. 9.472/97), a tutela de tais dados também não é absoluta, cedendo, por decisão judicial fundamentada ao interesse público (artigo 93, IX, da CF), desde que para fins de apurar fato que, em tese, configure ilícito penal, o que ocorre no presente caso. Assim, não há que se

falar em violação ao artigo 5º, inciso X, da Constituição Federal.

IX – Ordem denegada”[103].

Com efeito, em determinados casos, em que se exige segredo de justiça, poderá a autoridade não fornecer cópia da decisão aos responsáveis pelo provedor, que ainda assim, em tese, não poderiam se eximir de cooperar com as autoridades. Resta saber se tais entendimentos prevalecerão, com a recente aprovação do Marco Civil da Internet.

10.3. Busca e apreensão informática e perícia digital

As leis de crimes informáticos, logicamente, não tratam da busca e apreensão, instrumento cautelar muito útil na investigação de delitos informáticos. O instituto vem previsto nos arts. 240 e seguintes do Código de Processo Penal (Decreto-Lei n. 3.689, de 3-10-1941).

Sabemos que diante da suspeita de crimes cibernéticos, ou mesmo com base nos dados fornecidos pelos provedores ou responsáveis pelos ativos de TI, pode a autoridade requerer uma busca e apreensão na sede ou domicilio do suposto autor do delito, para que as máquinas sejam coletadas adequadamente para a realização de perícia técnica (para a apreensão de instrumentos utilizados na prática de crime ou destinados a fim delituoso).

A busca e apreensão informática segue logicamente a regra do Código de Processo Penal, sobretudo no que tange à necessidade dos agentes policiais preservarem o local do crime até a chegada dos peritos (art. 6º). A não observância destas regras pode constituir-se em nulidade.

Lembrando que as infrações informáticas deixam vestígios, razão pela qual é indispensável a realização do corpo de delito. Sabe-se que a prova pericial tem importância cada vez maior e sua realização deve se adequar a uma série de cuidados, sobretudo no que diz respeito à forma de realização. O exame de corpo de delito, em verdade, é perícia no escopo de se provar a materialidade de um crime. Em crimes informáticos, comumente o corpo de delito é direto, incidindo sobre os vestígios deixados pela infração. Excepcionalmente, pode ser indireto, quando os vestígios

desapareceram.

A busca e apreensão imprescinde de mandado judicial, nos termos do art. 243 do Código de Processo Penal[104]. É preciso que o mandado considere detalhes específicos da informática, como, por exemplo, a possibilidade de acesso a computadores remotamente administrados da localidade, dispositivos móveis em veículos ou em posse dos residentes, dentre outras características que a autoridade deve atentar para buscas desta natureza.

O sucesso da análise pericial está intimamente ligado com as cautelas adotadas na fase de busca e apreensão e coleta de evidências. O Código de Processo Penal classifica como nulidade insanável a falta do corpo de delito nos crimes que deixam vestígios. Tem-se como regra que o exame de corpo de delito seja feito (por peritos oficiais ou leigos, nomeados por juiz ou autoridade policial), antes da denúncia, porém nada impede que seja realizado durante o processo, logicamente com laudo juntado antes da sentença.

Destaca-se, pois, a importância da busca e apreensão para a apuração da materialidade e autoria de delitos informáticos.

Por fim, deve-se registrar que o acesso a mensagens ou *e-mails* contidos em dispositivo apreendido em busca e apreensão regularmente expedida não caracteriza interceptação de telecomunicações, senão vejamos:

"A simples verificação dos números das últimas chamadas feitas e recebidas constantes na memória do telefone celular não significa, por si só, violação ao sigilo telefônico desde que a apreensão do aparelho seja legítima. A garantia constitucional da inviolabilidade das comunicações telefônicas se refere à vedação de escutas clandestinas, a qual não se configura com a simples checagem dos últimos números registrados na memória do aparelho, ainda que esta seja realizada por outra pessoa que não o proprietário"[105].

10.4. Cooperação internacional

A tecnologia da informação integrou o mundo em uma grande teia, onde todos têm acesso a tudo, pouco importando o local físico em que realmente esteja armazenado tal conteúdo. Ocorre que, para a Justiça, o local físico da prática de um ato digital tem relevância para determinar a competência judiciária.

Não incomum, os agentes buscam praticar delitos por meio de sistemas hospedados no exterior. Nestes casos, a investigação, no Brasil, necessita da cooperação de provedores (de serviços e de conexão) de fora do país, o que não é uma tarefa fácil, considerando que parte dos provedores costuma alegar que não estão sujeitos às ordens da jurisdição brasileira (isto passa a se relativizar com a aprovação do Marco Civil da Internet).

Ocorre que não restam dúvidas de que a cooperação internacional é fundamental para o combate aos crimes cibernéticos. Na Europa, o G8 (grupo dos oito países mais industrializados) concebeu e administra a rede de cooperação denominada “Rede 8 x 7”, expandida para outros países como o Brasil, e disponível para autoridades policiais[106].

Em termos judiciais, em verdade, para que uma autoridade brasileira consiga dados relativos a usuários que usaram de serviços no exterior, o meio mais usual é a morosa “carta rogatória”, considerando que não se deve produzir prova ilícita, como o lançamento de “iscas” ou “*trojans* forenses”. Também existe o chamado “auxílio direto”, sendo que cada país adota uma forma de cooperação.

Em alguns casos, autoridades se valem do chamado DRCI do Ministério da Justiça, o Departamento de Recuperação de Ativos e Cooperação Internacional da entidade, que faz a intermediação entre órgãos judiciais dos países envolvidos.

Neste caso, o delegado que está conduzindo a investigação representa ao juiz, e de posse da resposta do juiz autorizando a quebra, ele entra em contato com o DRCI. Este, por sua vez, pode devolver a solicitação ao delegado, para que ela seja adaptada às necessidades do país que receberá a solicitação ou, caso esteja tudo em ordem e na língua do Estado de destino, encaminha ao país onde

se buscam os dados de um criminoso digital ou a remoção de um conteúdo ilícito.

Os dados, então, caso haja a cooperação, voltam ao DRCI, que comunica nos autos a informação, ou caso em fase de inquérito, diretamente à delegacia de polícia[107].

Esta cooperação é possível por ser o Brasil signatário do MLAT. A possibilidade do uso das cartas do chamado MLAT (*Mutual Legal Assistance Treaty*) não deve ser desconsiderada[108]. Por outro lado, tais procedimentos são absolutamente morosos, e muitas vezes os dados são excluídos rapidamente pelos provedores, e crimes eletrônicos podem ficar sem apuração, por ausência de provas ou exame de corpo de delito[109].

Deste modo, a cooperação internacional ainda é um desafio para a eficácia do combate ao crime eletrônico. Os provedores, como “portas” de entrada e saída da Internet, são os primeiros a ter a possibilidade de apurar dados de usuários que sejam seus clientes. Não bastasse, no que tange a provimento de aplicações e serviços, é notório que os serviços mais utilizados no Brasil pertencem a grandes provedores de conteúdo com sede no exterior (alguns, sequer com filiais físicas no Brasil). Neste contexto, em defesas envolvendo processos de quebras de sigilo de seus usuários, no Brasil, quase sempre argumentam que não estão sujeitos à jurisdição brasileira, apresentando inclusive a “lei do país sede”[110]. Muito embora tal argumentação seja desconsiderada pelo Judiciário na grande maioria dos casos, ainda preocupa a questão do provedor no exterior que não tem filial no Brasil[111]. Nestes casos, é importante que a cooperação internacional efetivamente se desenvolva[112].

11.

PERSPECTIVAS FUTURAS

O Governo de São Paulo anunciou em 2001 a criação de uma divisão da polícia para atender a crimes informáticos, na época, ainda sem legislação específica. Era criada a divisão de delitos praticados por meios eletrônicos da DIG (Delegacia de Investigações Gerais), a princípio para se especializar no combate aos crimes praticados por *crackers*. Hoje, esta delegacia é a DIG-DEIC, 4ª Delegacia de Repressão aos Crimes de Informática de São Paulo.

Neste tempo, muitas delegacias foram se estruturando[113]. Atualmente, em que pese a Lei n. 12.737/2012, é fato que a prova eletrônica constitui uma das principais barreiras para o sucesso da persecução criminal.

A Perícia Forense Digital precisará acompanhar as normas materiais. Provas virtuais necessitam ser confiáveis, reproduzíveis e, neste cenário, para serem aceitas juridicamente, devem passar por rigorosa perícia técnica, sob pena de nulidades processuais.

O novo Direito Digital impõe a necessidade de autoridades se atualizarem, em questões de tecnologia, para que possam efetivamente aplicar as normas sancionadas, fazendo frente ao crime eletrônico e proporcionando uma sociedade da informação minimamente segura, sem forçosos enquadramentos.

No que tange à prisão, em nossa ótica esta não se revela a medida mais adequada a lidar com criminosos desta natureza. Em verdade, pela nova Lei das prisões (Lei n. 12.403, de 4-5-2011), torna-se difícil que um *cracker* possa ser preso preventivamente. Já diante da condenação, entendemos que a tais meliantes podem ser aplicadas penas envolvendo prestação de serviços de segurança da informação e blindagem de sistemas. Segundo Patrícia Peck Pinheiro (2014, p. 313),

"colocá-lo simplesmente na cadeia junto a criminosos comuns é uma irresponsabilidade pública, já que pode provocar a criação de supercriminosos, o que é muito pior – mais ou menos o que ocorreu quando a ditadura brasileira colocou prisioneiros políticos junto com criminosos comuns...".

E mais, deve-se alertar, segundo Roza (2007, p. 73), que "é imperioso frisar, por derradeiro, que nenhum combate sério aos 'crimes de informática' se esgota no processo tipificador. Sem cooperação internacional, sem a melhoria do aparelhamento policial e sem o aperfeiçoamento profissional dos que operam nessas áreas, a simples existência de uma adequada tipificação não tem o menor significado prático e não basta para tutelar a sociedade contra tão lesiva atividade criminosa".

11.1. A reforma do Código Penal (PLS n. 236/2012) e os crimes cibernéticos

Em 27 de junho de 2012, o anteprojeto que propõe a Reforma do Código Penal foi entregue ao presidente do Senado. A proposta foi elaborada por juristas e tramita no Congresso Nacional como PLS n. 236/2012. O Anteprojeto foi apresentado ao então Presidente do Senado José Sarney e foi fruto de sete meses de discussões de uma Comissão de Juristas. Apesar da ampla discussão, ainda assim é considerado um projeto repleto de falhas, o que indica que longe está de aprovação.

Durante o trâmite, o Projeto já recebeu mais de 30 mil sugestões de setores da sociedade civil e entidades, tendo ainda recebido mais de 350 emendas. Não restam dúvidas de que a discussão só está começando, de maneira que é muito precoce para tratarmos seus reflexos em relação aos crimes cibernéticos.

A despeito deste fato, é possível já visualizar os pontos que a reforma do Código Penal traz em relação aos crimes cibernéticos. Muitas das propostas em relação a cibercrimes são incompatíveis considerando as leis já existentes. Outras ainda carecerão de maiores estudos, pois são genéricas e com possibilidade de amplas interpretações.

Inicialmente, na Parte Especial do Projeto do novo Código Penal, temos, na última versão do Projeto de Lei do Senado n. 236/2012, o Título VI, que trata dos crimes cibernéticos, trazendo

(numeração dos artigos pode mudar, considerando se tratar de um projeto de lei):

a) No art. 208 uma conceituação, envolvendo “sistema informático”, “dados informáticos”, “provedor de serviços” e “dados de tráfego”, assim classificando: “sistema informático”: qualquer dispositivo ou o conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção; “dados informáticos”: qualquer representação de fatos, informações ou conceitos sob forma suscetível de processamento num sistema informático, incluindo programas aptos a fazerem um sistema informático executar uma função; “provedor de serviços”: qualquer entidade, pública ou privada, que faculte aos utilizadores de seus serviços a capacidade de comunicação por meio de seu sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome desse serviço de comunicação ou de seus utentes; “dados de tráfego”: dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

b) No art. 209, conceituando o delito de “acesso indevido”, com a conduta de “acessar, indevidamente ou sem autorização, por qualquer meio, sistema informático protegido, expondo dados informáticos a risco de divulgação ou de utilização indevida”, punindo também aquele que, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa ou por qualquer forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a ação descrita no tipo penal. A pena prevista é de prisão de seis meses a um ano e multa.

Neste tipo penal existe também uma causa de aumento da pena, de um sexto a um terço, se do acesso resultar prejuízo econômico. Igualmente, assim como na Lei n. 12.737/2012, o Projeto prevê

como causa de aumento de pena, de um a dois terços, se houver divulgação, comercialização ou transmissão dos dados ou informações obtidos.

Existe uma qualificadora no tipo do art. 209 do Projeto de Lei do Senado n. 236/2012, em que a pena é de dois a quatro anos, se o crime é cometido contra Administração Pública direta ou indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos.

O Projeto prevê também no delito de "acesso indevido", a qualificadora se do acesso resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo acessado. Nestas hipóteses, a pena é de prisão de um a dois anos.

O art. 209 certamente não será aprovado ou mantido no Projeto de Lei do Senado n. 236/2012, considerando ser incompatível com o delito previsto no art. 154-A do Código Penal, trazido pela Lei n. 12.737/2012, já em vigor.

c) No art. 210, o delito de "sabotagem informática", punindo aquele que interfere de qualquer forma, indevidamente ou sem autorização, na funcionalidade de sistema informático ou de comunicação de dados informáticos, causando-lhe entrave, impedimento, interrupção ou perturbação grave, ainda que parcial, com uma pena de prisão de um a dois anos, sendo que na mesma pena incorre quem, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa ou por qualquer outra forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a sabotagem informática. Tipo que reputamos importante para suprir lacuna da Lei n. 12.737/2012 em relação à sabotagem de ativos de particulares.

Do mesmo modo, se o crime é cometido contra a Administração Pública direta ou indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos, a pena é de prisão, de dois a quatro anos.

Embora não sejam tipos idênticos, o Projeto do Novo Código Penal trouxe em seu art. 266 o delito

de “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”. Porém, aqui protege-se a coletividade.

Além das disposições sobre crimes cibernéticos (crimes próprios – onde o sistema informático é o bem ofendido), outras inserções/alterações são promovidas no Código Penal, com o Projeto de Lei do Senado n. 236/2012, ainda em trâmite no Congresso, as quais terão relevância para o estudo dos crimes informáticos impróprios (onde a informática é o meio para a prática de crimes). Vejamos as principais alterações propostas ao Código Penal.

a) Cria-se o delito de “terrorismo”, previsto dentre os crimes contra a paz pública, em seu art. 239, punindo aquele que causa terror na população, mediante várias condutas, dentre as quais interferir, sabotar ou danificar sistemas de informática e bancos de dados. Comina pena de prisão de oito a quinze anos; Este tipo precisará de maiores reflexões para se compatibilizar com o delito previsto no art. 154-A do Código Penal, em vigor com a Lei Carolina Dieckmann.

b) Dentre os Crimes contra a Administração Pública, insere o delito “Modificação ou alteração não autorizada de sistemas de informações”, no art. 274, punindo o funcionário que assim procede, causando dano para a Administração Pública ou administrado, com pena de prisão de três meses a dois anos. Tal delito precisará ser refletido em cotejo com os arts. 313-A e 313-B do Código Penal, inseridos pela Lei n. 9.983/2000.

c) Dentre a seção “Dos crimes contra as crianças e adolescentes”, cria o delito de “Divulgação de cena de sexo”, envolvendo criança e/ou adolescente, inclusive por meio informático, cominando pena de prisão de três a seis anos. Ocorre que o Estatuto da Criança e do Adolescente, em seu art. 241-A, modificado pela Lei n. 11.829/2006, já traz tipo penal semelhante, prevendo pena de reclusão de três a seis anos e multa.

d) Cria no art. 17 do Código Penal o delito de “Fraude informática”, previsto dentre os crimes contra o patrimônio, para punir aquele que adultera dados informáticos para obter para si ou para outrem vantagem ilícita, em prejuízo alheio, trazendo uma pena de prisão de um a cinco anos. Tal

delito precisará ser refletido e compatibilizado com os delitos já existentes no Código Penal, como o do art. 299 (falsidade ideológica) e até mesmo em relação ao art. 171 (estelionato).

e) No art. 172, traz o delito de "Violação de direito autoral", que por sua vez é qualificado no § 2º para aquele que distribui conteúdo protegido por meio da informática, com intuito de lucro direto ou indireto, trazendo uma pena para a forma qualificada de prisão de um a quatro anos. Uma adaptação ao delito do atual art. 184 do Código Penal.

f) No art. 151, que trata do delito de violação de correspondência, previsto dentre os crimes contra a inviolabilidade de correspondência, tem-se a inserção de uma forma qualificada, quando o agente comete o crime com abuso de função em serviço postal, telegráfico, telefônico ou em provedor de serviço de comunicação ou de tratamento de dados informáticos. Nestes casos, a pena será de prisão de um a três anos. Disposição até então inexistente no ordenamento penal brasileiro.

g) No art. 153 do Código Penal, delito de divulgação de segredo, previsto dentre os crimes contra a inviolabilidade dos segredos, acrescenta-se a forma qualificada, no § 1º, para o caso de divulgação, sem justa causa, de informações privadas ou reservadas, contidas ou não em sistemas informáticos ou bancos de dados, trazendo uma pena de um a quatro anos de prisão. Existindo ainda uma causa de aumento para os casos em que o agente pratica quaisquer das condutas do *caput* mediante o uso de rede social ou através de sistema informático que facilite ou amplie a consumação do delito, onde a pena será aumentada de um a dois terços. Pune-se a divulgação por meio potencializador, como a Internet.

h) É criado o art. 14, trazendo o tipo penal da "Interceptação ilícita", dentre os crimes contra a inviolabilidade dos segredos, punindo quem intercepta comunicações telefônicas, telemática ou ambiental, sem autorização judicial, com pena de prisão de dois a cinco anos, punindo ainda, com aumento de pena de um terço até a metade, aquele que revela o conteúdo interceptado, por vários meios, inclusive a Internet.

i) No art. 155, crime de furto, é acrescentado um § 1º que expressamente equipara à coisa móvel

sinal de Internet ou item assemelhado que tenha valor econômico, trazendo nova pena de seis meses a três anos (pena menor que a do atual Código Penal). Este tipo precisa de muitas reflexões, pois é muito “aberto”, podendo ser interpretado de modo a prejudicar o acusado.

j) É criado o art. 164, prevendo o delito de “Dano a dados informáticos”, inerente à conduta daquele que destruir dados informáticos ou distribuir programas ou dados destinados a destruição. A pena é de prisão de seis meses a três anos. Importante tipo penal, pois resolverá a polêmica relativa à possibilidade de dados sofrerem danos.

k) Introduz o delito previsto no art. 472, que vem a substituir a Lei n. 7.716/89, tratando do crime de “racismo”, previsto no Capítulo V do Projeto de Código Penal, envolvendo o título “Do racismo e dos crimes resultantes de preconceito e discriminação”, punindo aquele que também praticar, induzir ou incitar a discriminação ou preconceito, pela fabricação, comercialização, veiculação e distribuição de símbolos, emblemas, ornamentos, distintivos ou propaganda que a indiquem, inclusive pelo uso de meios de comunicação e Internet.

Em apertada síntese, estas são as principais propostas relacionadas à questão dos crimes informáticos trazidas por ocasião da apresentação do Projeto de Lei de Reforma do Código Penal, ainda em trâmite. Como se pode prever, certamente, muitos pontos mudarão e serão suprimidos, considerando que a fase de debates está se iniciando nas Casas de Leis. Ainda assim, tal conteúdo é importante ao operador do Direito Penal Informático, na medida em que poderá se preparar de imediato para o futuro envolvendo a tipificação de novos delitos cibernéticos, bem como a adequação de velhos tipos para se fazer frente a situações delituosas envolvendo a tecnologia da informação.

Em 17 de dezembro de 2014 foi apresentada versão final do PLS n. 236/2012 no Senado[114], que traz significativas mudanças e ajustes à versão original proposta e que aqui foi tratada. Entre essas mudanças, citamos as mais relevantes, resumidamente:

a) Cria o tipo de “Distribuição de material produzido com violação de direito autoral”, incluindo o

programa de computador, prevendo pena de prisão de dois a cinco anos;

b) No capítulo envolvendo os crimes cibernéticos, cria o tipo da "Fraude informatizada", com prisão de um a cinco anos para aquele que obtém, para si ou para outrem, em prejuízo alheio, vantagem ilícita, mediante a introdução, alteração, supressão ou captura de dados informatizados, ou pela interferência indevida, por qualquer outra forma, no funcionamento de sistema informatizado;

c) Cria os tipos de "Obtenção indevida de credenciais de acesso", punindo aquele que adquirir, obtiver ou receber indevidamente credenciais de acesso a sistema informatizado, com pena de prisão de um a três anos;

d) Cria o crime de "artefato malicioso", punindo quem desenvolve código e programas maliciosos, mas excetuando a atividade de pesquisa, assim descrito: *Produzir, adquirir, obter, vender, manter, possuir ou por qualquer forma distribuir, sem autorização, artefatos maliciosos destinados à prática de crimes previstos neste Título:*

> *Pena – a prevista para o crime fim, sem prejuízo da aplicação das regras do concurso material.*
>
> *Excludente de ilicitude*
>
> *Parágrafo único. Não são puníveis as condutas descritas no* caput *quando realizadas para fins de:*
>
> *I – investigação por agentes públicos no exercício de suas funções;*
>
> *II – pesquisa acadêmica;*
>
> *III – testes e verificações autorizadas de vulnerabilidades de sistemas; ou*
>
> *IV – desenvolvimento, manutenção e investigação visando ao aperfeiçoamento de sistemas de segurança.*

e) Estabelece no delito de "Fraude contra falência ou recuperação judicial ou extrajudicial" a pena de prisão de três a seis anos para aquele que destrói, apaga ou corrompe dados contábeis ou negociais armazenados em computador ou sistema informatizado;

f) Estabelece o crime de "Divulgação de cena de sexo", punindo com pena de prisão de três a seis anos aquele que assegura, por qualquer meio, o acesso por rede de computadores a fotografias, cenas ou imagens, vídeo ou outro registro que contenham cena de sexo explícito ou pornográfica envolvendo criança ou adolescente;

g) No crime de furto estabelece a mesma pena para aquele que utiliza de artifício para a captação

de sinal de comunicação audiovisual de acesso condicionado, de Internet ou assemelhado, que tenha valor econômico, sem a devida contraprestação financeira;

h) Estabelece o delito de "Interceptação ilícita", este envolvendo as comunicações eletrônicas, com pena de prisão de dois a cinco anos e com aumento de pena de metade se a divulgação ilícita for feita por meio da imprensa, rádio, televisão, Internet ou qualquer outro meio que facilite a sua propagação;

i) Cria o tipo penal de "Perseguição obsessiva ou insidiosa", com pena de prisão de dois a seis anos para aquele que perseguir alguém, de forma reiterada ou continuada, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a liberdade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. No entanto, o projeto silencia em relação à perseguição pela Internet, o chamado "stalking".

Recomenda-se aos profissionais a constante pesquisa no *site* do Senado Federal, para acompanhamento do trâmite legislativo do Projeto de Lei do Senado n. 236/2012[115].

11.2. O Projeto de Lei n. 7.758/2014

Está em vigor na Câmara dos Deputados o Projeto de Lei n. 7.758/2014[116] que pretende tipificar penalmente o uso de falsa identidade através da Internet. O escopo é alterar o crime de falsa identidade do Código Penal, que criminalizará também aqueles que usam a Internet com o objetivo de intimidar, prejudicar, ameaçar, obter vantagem ou causar dano a outra pessoa, em proveito próprio ou alheio. Dispõe a proposta:

Art. 307. Atribuir-se ou atribuir a terceiro falsa identidade, inclusive por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio:

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave.

Não se alterando a pena, o crime continua sendo punido com três meses a um ano de detenção, ou multa, se o fato não constituir elemento de crime mais grave. Trata-se de projeto de lei que pode complementar a Lei n. 12.737/2014, criminalizando o uso de "perfil falso" na rede mundial de computadores.

Entendemos que a proposta não tem a menor razão de existir, primeiro, porque o delito do art. 307 do Código Penal, como está, já faz frente àquele que usa perfil falso na Internet. Além disso, pela proposta não se alterou a pena para o delito e o interessante seria o agravamento da pena em casos de Internet. Não bastasse, o Projeto de Lei n. 7.758/2014 dispõe que o objetivo do perfil falso deve ser o de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem. Aquele que criasse um perfil falso humorístico, por exemplo, seria punido. Ademais, "prejudicar" é expressão por demais vaga, podendo restar em interpretações forçosas.

CONCLUSÕES

Não foi pretensão dos autores trazer respostas para as questões envolvendo a Lei de Crimes Informáticos. Pelo contrário, o escopo foi propor reflexões, apresentar as divergências de entendimentos e os desafios futuros. Foi possível, com a presente obra, fazer uma ponte entre o mundo técnico e da segurança da informação e legal nas questões envolvendo crimes cibernéticos, aprofundando os estudos sobre o tema, sempre com um olhar envolvendo a segurança da informação, em prestígio aos profissionais da área, poucas vezes ouvidos em processos legislativos como o presente, que resultaram da aprovação das Leis n. 12.735/2012 e 12.737/2012. Como se verificou, vivemos uma globalização e o desafio de lidarmos com crimes cada vez mais transnacionais.

As leis ora estudadas já estão em vigor, e logo teremos os julgados a respeito das temáticas neste livro vislumbradas. O Judiciário deve apreciar questões complexas, tendo bom senso para evitar decisões incorretas e contraditórias. Foi escopo deste trabalho auxiliar autoridades de aplicação de lei e operadores do Direito nesta difícil tarefa. Igualmente, o livro, explorando questões técnicas polêmicas e corriqueiras, apresenta-se como um guia a profissionais de tecnologia e segurança da informação em geral, para que possam desenvolver suas atividades nos termos da lei, sobretudo que sejam investigadores e questionadores, não aceitando imposições de quem desconhece os detalhes da tecnologia da informação.

Muito temos a caminhar. O desafio está sempre começando, se renovando, sobretudo com o Projeto de Reforma do Código Penal. Mas já avançamos muito com as edições das Leis de Crimes Informáticos (n. 12.737/2012) e Marco Civil da Internet (n. 12.965/2014), trazendo este a obrigatoriedade da guarda de registros de conexão ou acesso a aplicações, regulamentando também o acesso, por autoridades administrativas, aos dados cadastrais de um indiciado ou investigado.

A presente obra será atualizada de acordo com a evolução dos entendimentos e posicionamentos jurisprudenciais e doutrinários. Não se trata da palavra final. Seja como for, não se pode mais negar

a importância de conhecimento tecnológico na vida do advogado e aplicador do Direito, como condição para que possa desenvolver suas atividades com excelência e justiça, eis que, segundo Renato Borruso (1989, p. 29), *"se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista. Será o fim do Estado de Direito e a democracia se transformará facilmente em tecnocracia"* [117].

Finalizamos salientando que a cooperação internacional continua sendo essencial, dadas as características da rede, que permitem que agente e vítima estejam em países distintos ou tenham nacionalidades distintas. A cooperação internacional poderá refletir em uma uniformização mínima das leis, bem como a efetiva comunicação judicial e policial e uma padronização dos registros e *logs*, sendo pois possível repreender o crime cibernético, pouco importando a nacionalidade dos envolvidos ou o local da ação ou omissão e do resultado.

Com esta obra, nos contentamos se pudemos demonstrar que legislar sobre crimes informáticos não é tarefa tão simples quanto parece. Mais que isso, demonstrando as diversas interpretações cabíveis às leis de crimes informáticos, evidenciamos que, tão difícil quanto legislar sobre tecnologia e Internet em matéria criminal, será assentar ou pacificar as diversas óticas e entendimentos sobre as precitadas leis, agora em vigor no Brasil desde 2013. Que a história possa ser considerada, quando se pensar, novamente, na elaboração de novas leis de crimes cibernéticos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2006.

BAKER, Stewart. *Aaron Swartz's Impact on New Computer Fraud and Abuse Act Proposal is Clear*. Disponível em: <http://www.opposingviews.com/i/politics/dubious-proposal-amending-computer-fraud-and-abuse-act#> Acesso em: 7 maio 2014.

BEAL, Adriana. *Segurança da informação*: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BELL, D. *O advento da sociedade pós-industrial*: uma tentativa de previsão social. São Paulo: Cultrix, 1979.

BLUM, Renato Opice. *Crimes eletrônicos*: a nova lei é suficiente? Disponível em: <http://www.fecomercio.com.br/crimeseletronicos/2013/01/artigo-crimes-eletronicos-a-nova-lei-e-suficiente-por-renato-opice-blum/>. Acesso em: 7 maio 2014.

BORRUSO, Renato. *Computer e diritto II*. Milão: Giuffrè, 1989.

BOTTINI, Pierpaolo Cruz. *Crime de perigo abstrato*. Disponível em: <http://www.btadvogados.com.br/pt-br/content/crime-de-perigo-abstrato>. Acesso em: 7 maio 2014.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da República Federativa do Brasil*. Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 abr. 2014.

BRASIL. Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras

providências. *Diário Oficial da República Federativa do Brasil*. Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 28 abr. 2014.

BRASIL. Lei n. 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei n. 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. *Diário Oficial da República Federativa do Brasil*. Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 28 abr. 2014.

BRASIL. Lei n. 6.996, de 7 de junho de 1982. Dispõe sobre a utilização de processamento eletrônico de dados nos serviços eleitorais e dá outras providências. *Diário Oficial da República Federativa do Brasil*. Brasília, DF, 23 abr. 2014. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/1980-1988/L6996.htm>. Acesso em: 28 abr. 2014.

BRASIL. Lei n. 4.737, de 15 de julho de 1965. Institui o Código Eleitoral. *Diário Oficial da República Federativa do Brasil*. Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L4737.htm#art315>. Acesso em: 28 abr. 2014.

BRIAT, Martine. La fraude informatique: une approche de droit compare. *Revue de Droit Pénal et Criminologie,* Bruxelles, n. 4, 1985.

BRITO, Auriney. *Direito penal informático*. São Paulo: Saraiva, 2013.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei 12.737/12 e o crime de invasão de dispositivo informático. *Universo Jurídico*, Juiz de Fora, ano XI, 5 fev. 2013. Disponível em: <http://uj.novaprolink.com.br/doutrina/9014/primeiras_impressoes_sobre_a_lei_12_73712_e_o_crir Acesso em: 10 maio 2014.

________. O novo crime de invasão de dispositivo informático. *Consultor Jurídico*. Disponível em:

<http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 7 maio 2014.

CÂMARA DOS DEPUTADOS. PL 84/99. Brasília, DF, 24 fev. 1999. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em: 7 maio 2014.

CARVALHO, Ivan Lira de. Crimes na Internet. Há como puni-los. *Jus Navigandi*, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus.com.br/revista/texto/2081>. Acesso em: 7 maio 2014.

CARVALHO, Maria Augusta. Marco Civil brasileiro para a Internet já é copiado no exterior. Disponível em: <http://www.conjur.com.br/2014-set-02/marco-civil-brasileiro-internet-copiado-exterior>. Acesso em: 10 jan. 2015.

CARTILHA DE SEGURANÇA PARA A INTERNET. *Cert.br*. Disponível em: http://cartilha.cert.br/glossario/. Acesso em: 12 maio 2014.

CASTELLA, Eduardo Marcelo. *Investigação criminal e informática*. Curitiba: Juruá, 2005.

CASTELLS, Manuel. *A galáxia da Internet*: reflexões sobre a Internet, os negócios e a sociedade: Rio de Janeiro: Zahar, 2003.

CAVALCANTE, Márcio André Lopes. Comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. *Atualidades do Direito*, 9 jan. 2013. Disponível em: <http://atualidadesdodireito.com.br/marciocavalcante/2013/01/09/comentarios-a-lei-12-7372012-que-tipifica-a-invasao-de-dispositivo-informatico/>. Acesso em: 7 maio 2014.

________. *Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático*. Disponível em: <http://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 7 maio 2014.

COMPUTER Fraud & Abuse Act. Disponível em: <http://cio.energy.gov/ComputerFraud-AbuseAct.pdf>. Acesso em: 6 ago. 2014.

COMPUTER Misuse Act 1990. *Wikipedia.* Disponível em:

<http://en.wikipedia.org/wiki/Computer_Misuse_Act_1990>. Acesso em: 30 jan. 2014.

CONVENÇÃO SOBRE O CIBERCRIME. Conselho da Europa. Budapeste, 23 nov. 2001. *Council of Europe*. Disponível em: <http://conventions.coe.int/treaty/EN/Treaties/PDF/185-POR.pdf>. Acesso em: 23 abr. 2014.

CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011.

CRIMES de Informática serão tratados em lei específica. São Paulo. OAB/SP, 1999. Disponível em: <http://www2.oabsp.org.br/asp/clipping_jur/ClippingJurDetalhe.asp?id_noticias=5406&AnoMes=19991>. Acesso em: 7 maio 2014.

CRIMES virtuais que viraram notícia. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u19460.shtml>. Acesso em: 13 jan. 2014.

DAOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato M. S. Opice (coord). *Direito eletrônico:* a internet e os tribunais. Bauru: Edipro, 2001.

DAVARA RODRIGUÉS, Miguel Ángel. *Código de Internet*. Pamplona: Aranzadi, 2002.

DIÁRIO NACIONAL. STJ de 8-8-2012 (7670970). Disponível em: <http://www.radaroficial.com.br/d/7670970>. Acesso em: 7 maio 2014.

FABBRINI, Renato; MIRABETE, Julio Fabbrini. *Manual de direito penal.* São Paulo: Atlas, 2014. v. 1.

FENSEG. Brasil na rota de crimes cibernéticos. Disponível em: <http://www.cnseg.org.br/fenseg/servicos-apoio/noticias/brasil-na-rota-de-crimes-ciberneticos.html>. Acesso em: 22 jun. 2015.

FERREIRA, Érica Lourenço de Lima. *Criminalidade econômica e empresarial e cibernética.* Florianópolis: Momento Atual, 2005.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (orgs.). *Direito & internet*: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

________. Os "crimes de informática". In: BARRA, Rubens Prestes; ANDREUCCI, Ricardo

Antunes. *Estudos jurídicos em homenagem a Manoel Pedro Pimentel.* São Paulo: Revista dos Tribunais, 1992.

GARCIA, Flúvio Cardinelle Oliveira. Da validade jurídica dos contratos eletrônicos. *Jus Navigandi*, Teresina, ano 9, n. 264, 28 mar. 2004. Disponível em: <http://jus.com.br/artigos/4992>. Acesso em: 7 maio 2014.

GERSCHENFELD, Ana. *A Internet está a mudar a nossa forma de pensar?* Disponível em: <http://www.publico.pt/tecnologia/noticia/a-internet-esta-a-mudar-a-nossa-forma-de-pensar-1416806>. Acesso em: 10 jan. 2015.

GLOSSÁRIO DE SEGURANÇA MICROSOFT. *Microsoft.* Disponível em: <http://www.microsoft.com/brasil/security/glossary.mspx>. Acesso em: 12 maio 2014.

GONZAGA, Yuri. "Sociabilidade" do brasileiro propicia crimes virtuais, diz empresa; prejuízo aumenta. Disponível em: <http://www1.folha.uol.com.br/tec/2013/12/1385479-sociabilidade-do-brasileiro-propicia-crimes-virtuais-diz-empresa-saiba-se-proteger.shtml>. Acesso em: 22 jun. 2015.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. *Boletim IBCCrim,* São Paulo, ed. esp., ano 8, n. 95, out. 2000.

HERRERO, Cesar. *Los delitos económicos:* perspectiva jurídica y criminológica. Madrid: Ministerio del Interior, Secretaria Geral Tecnica, 1992.

HULETTE, Elisabeth. *Police can require cellphone firgerprint, not pass code*. Disponível em: <http://hamptonroads.com/2014/10/police-can-require-cellphone-fingerprint-not-pass-code>. Acesso em: 15 jan. 2015.

ÍNDICE do dicionário técnico. *Guia do hardware.* Disponível em: <http://www.hardware.com.br/termos/>. Acesso em: 12 maio 2014.

JAKOBS, Günther. *A imputação objetiva no direito penal*. 2. ed. rev. Trad. André Luis Callegari. São Paulo: Revista dos Tribunais, 2007.

JESUS, Damásio E. *Novas questões criminais.* São Paulo: Saraiva, 1993.

JOSEPH-MARIE_JACQUARD. *Wikipedia.* Disponível em: <http://pt.wikipedia.org/wiki/Joseph-Marie_Jacquard>. Acesso em: 30 jan. 2014.

KURTZ, João. Registros de ocorrências de crimes virtuais aumentam 70% no país em 1 ano. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2014/10/registros-de-ocorrencias-de-crimes-virtuais-aumentam-70-no-pais-em-1-ano.html>. Acesso em: 10 jan. 2014.

LEVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999.

LIMA, Paulo Marcos Ferreira. *Crimes de computador e segurança computacional*. São Paulo: Atlas, 2011.

MCLUHAN, H. M. *Understantig Media*: The Extensions of Man. New York: The New America Library, 1964.

McLUHAN, Marshall. *Understanding Media*. Routledge, London, 1964.

MILAGRE, José Antonio. *Usuários podem instalar programa e alistar suas máquinas para a Guerra Virtual*. Disponível em: <http://josemilagre.com.br/blog/wp-content/uploads/2011/10/Artigo-Usuarios-podem-instalar-programa-e-alistar-suas-maquinas-para-Guerra-Virtual-Jose-Milagre-08-01-11.pdf>. Acesso em: 7 maio 2014.

________. Invasão de dispositivo com senha nem sempre é crime. *Consultor Jurídico*, 1 abr. 2013. Disponível em: <http://www.conjur.com.br/2013-abr-01/jose-milagre-invasao-dispositivo-senha-nem-sempre-crime>. Acesso em: 7 maio 2014.

NERY, Claudio Lima; BITTENCOURT, Manoela; AZAMBUJA, Mariana Menna Barreto. *A proteção de dados pessoais e a Internet*. Disponível em: <http://www.tex.pro.br/home/artigos/258-artigos-dez-2013/6364-a-protecao-de-dados-pessoais-e-a-internet-the-personal-data-protection-and-the-internet>. Acesso em: 7 maio 2014.

8 de cada 10 hackers vivem no Brasil, diz PF. São Paulo. *Info Online*, 2004. Disponível em: <http://info.abril.com.br/aberto/infonews/092004/13092004-13.shl>. Acesso em: 7 maio 2014.

Open Web Application *Security* Project (OWASP). *OWASP Top Ten Project*. Disponível em:

<https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>. Acesso em 10 jan. 2015.

Perdas com cibercrimes chegam a R$ 15 bilhões no Brasil por ano. Disponível em: <http://www.teletime.com.br/04/10/2012/perdas-com-cibercrimes-chegam-a-r-15-bilhoes-no-brasil-por-ano/tt/304178/news.aspx>. Acesso em: 15 jan. 2015.

PINHEIRO, Patrícia Peck. *Direito digital.* 2. ed. São Paulo: Saraiva, 2007.

________. *Direito digital.* 5. ed. São Paulo: Saraiva, 2014.

Projeto de Lei no Senado tenta modificar o Marco Civil. Disponível em: <http://olhardigital.uol.com.br/noticia/projeto-de-lei-do-senado-tenta-modificar-o-marco-civil/43759>. Acesso em: 15 jan. 2014.

RAMOS, Guilherme da Rocha. Princípio da consunção: o problema conceitual do crime progressivo e da progressão criminosa. *Jus Navigandi*, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: <http://jus.com.br/artigos/996>. Acesso em: 7 maio 2014.

ROHR, Altieres. Saiba o que são falhas de segurança “dia zero” e como se proteger delas. *Globo.com*. Data de publicação: 18-5-2009. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1128175-6174,00-SAIBA+O+QUE+SAO+FALHAS+DE+SEGURANCA+DIA+ZERO+E+COMO+SE+PROTEGER+D
Acesso em: 12 maio 2014.

ROQUE, Sérgio Marcos. Crimes de informática e investigação policial. In: PENTEADO, Jacques de Camargo et al (coords.). *Justiça penal.* 7. ed. São Paulo: Revista dos Tribunais, 2000.

ROSSETTO, Marcela. Direito penal mínimo na web. Revista *Visão Jurídica*, São Paulo. Disponível em: <http://revistavisaojuridica.uol.com.br/advogados-leis-jurisprudencia/62/artigo220896-4.asp>. Acesso em: 7 maio 2014.

ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal.* São Paulo: Memória Jurídica, 2004.

ROVIRA DEL CANTO, Enrique. *Delincuencia informática y fraudes informáticos.* Granada:

Comares, 2002.

ROZA, Fabrízio. *Crimes de informática.* 2. ed. Campinas: Bookseller, 2007.

RUSSO, Rafael. *Hacker Black Hat, White Hats e Gray Hats, qual a diferença?* Disponível em: <escreveassim.com.br/2013/04/22/hackers-black-white-grey-hat/http://www.teletime.com.br/04/10/2012/perdas-com-cibercrimes-chegam-a-r-15-bilhoes-no-brasil-por-ano/tt/304178/news.aspx>. Acesso em: 15 jan. 2015.

SCHJOLBERG, Stein. *The History of Global Harmonization on Cibercrime Legislation – The Road to Geneva.* Dez. 2008. Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>. Acesso em: 13 maio 2014.

SEARCH SECURITY. *Tech Target*. Disponível em: <http://searchsecurity.techtarget.com/definition/payload>. Acesso em: 12 maio 2014.

SIEBER, Ulrich. *Computer crime and criminal information law:* new tends in the international risk information society. Disponível em: <www.jura.uniwuerzburg.de\sieber>. Acesso em: 14 dez. 2007.

________. Criminalidad informática: peligro y prevención. In: MIR PUIG, Santiago (comp.). *Delincuencia informática.* Barcelona: PPU, 1992 (Iura n. 7).

________. Legal aspects of computer-related crime in the information society – Comcrime-Study. União Europeia. Universidade de Wüerzburg. Versão 1.0, jan. 1998. *Santa Clara Law*. Disponível em: <http://law.scu.edu/international/File/Sieber_final.pdf>. Acesso em: 29 abr. 2014.

________. *The international handbook on computer crime.* New York: John Wiley Sons, 1986.

SILVA, Mauro Marcelo de Lima e. *Os crimes digitais, hoje. Polícia revela o perfil do criminoso na Internet*. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/29333-29351-1-PB.htm>. Acesso em: 15. jan. 2014.

SILVA NETO, Amaro Moraes e. *Privacidade na internet*. São Paulo: Edipro, 2001.

SILVEIRA, Renato de Mello Jorge. *Direito penal supraindividual*: interesses difusos. São Paulo: Revista dos Tribunais, 2003.

TIEDEMANN, Klaus. *Lecciones de derecho penal económico*. Barcelona: PPU, 1993.

________. *Poder econômico y delito*. Trad. Amelia Mantilla Villegas. Barcelona: Ariel, 1985.

________. Criminalidad mediante computadores. In: *Poder Econômico y Delito*. Barcelona: Ariel, 1985.

TNU – HC 201103000101390. *Revista Jus Brasil*. Disponível em: <http://tnu.jusbrasil.com.br/jurisprudencia/20606584/hc-habeas-corpus-hc-201103000101390>. Acesso em: 7 maio 2014.

Trustwave global security report. Disponível em: <http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf?aliId=37614026>. Acesso em: 10 jan. 2015.

Unauthorized Computer Access Law. Disponível em: <http://www.cybercrimelaw.net/Japan.html>. Acesso em: 7 maio 2014.

VIANNA, Tulio; MACHADO, Felipe. *Crimes informáticos*: conforme a Lei n. 12.737/2012. Belo Horizonte: Fórum, 2013.

WIENER, Norbert. *Cibernética*: ou controle da comunicação no animal e na máquina. Trad. Gita K. Ghinzberg. São Paulo: Polígono, 1970.

WIKI UBUNTU BRASIL. *Ubuntu wiki*. Disponível em: <http://wiki.ubuntu-br.org/arpspoofing>. Acesso em: 12 maio 2014.

WIKIPEDIA, enciclopédia livre. *Wikipedia*. Disponível em: <http://pt.wikipedia.org/>. Acesso em: 12 maio 2014.

ZACLIS, Daniel. O vírus informático e o crime de dano: por que legislar? *Boletim IBCCrim*, São Paulo, ano 14, n. 173, p. 18-19, abr. 2007.

GLOSSÁRIO

Appliance: Ferramenta. As *Appliances* são computadores pré-configurados para executar uma tarefa específica, como servir para compartilhar a conexão com a *Web* ou como um *firewall* para a rede, como um *kiosque* multimídia, como um sistema de caixa registradora e leitor de código de barras, um centro de multimídia, um centro de controle de um sistema de automatização doméstica, dentre outros.

ARP Poisoning ou ARP Poison Routing: É a técnica utilizada em redes cabeadas e *wireless* que permite ao atacante capturar informações, modificar o tráfego ou bloqueá-lo causando DOS (*Denial of Service*).

Backdoor: Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio de inclusão de serviços criados ou modificados para este fim. Normalmente esse programa é colocado de forma a não ser notado.

Back-Orifice: *Trojan* que, uma vez instalado no micro da vítima, abre a máquina a acesso externo, permitindo quase tudo, até mesmo ejetar CDs ou resetar o micro remotamente. O *Back-Orifice* opera de forma muito semelhante aos programas de administração remota, com possibilidade de alterar a porta TCP escutada pelo programa, ou mesmo estabelecer uma senha de acesso.

BackTrack Linux: É focado em testes de segurança e testes de penetração (*pentests*), muito apreciada por *hackers* e analistas de segurança, podendo ser iniciado diretamente pelo CD (sem necessidade de instalar em disco), mídia removível (*pen drive*), máquinas virtuais ou direto no disco rígido.

BBSs: Do inglês ***B****ulleting* ***B****oard* ***S****ystems*. É um sistema informático, um *soft-ware*, que permite a ligação (conexão) via telefone a um sistema através do seu computador e interagir com ele, tal como hoje se faz com a Internet.

Binders: Um *software* ou utilitário que combina dois ou mais arquivos em um único arquivo. Para vincular arquivo, o usuário seleciona uma lista de arquivos a serem colocados em um arquivo que servirá de *host*, comprime os arquivos e os salva em um único arquivo. Quando o usuário clica no *host*, os arquivos incorporados são automaticamente descompactados e se contiverem um executável, tal arquivo será executado. O *software* é utilizado comumente para embutir cavalos de troia e códigos maliciosos.

Brutal force: Força bruta. Tipo de ataque que consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios desse usuário.

Cloud Computing: Computação em nuvens. Refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, seguindo o princípio da computação em grade.

Data loss prevention: Solução de prevenção contra perdas de dados, é um sistema concebido para detectar potenciais ou violações de dados por meio de monitoramento ou impedindo o acesso a informação em uso, sendo transmitida ou armazenada. Em síntese, é possível detectar e monitorar o fluxo de dados.

Defacement: Desfiguração, deformação, obliteração, mutilação. Termo de origem inglesa para o ato de modificar ou danificar a superfície ou aparência de algum objeto. Na segurança da informação, é usado para categorizar os ataques realizados por *defacers* e *script kiddies* para modificar a página de um sítio na Internet. Também chamada de pichação. Técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

Denial of Service: Atividade maliciosa, coordenada e distribuída, pela qual um conjunto de computadores e/ou dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Dictionary attack: Ataque de dicionário. Ataque que consiste na cifragem das palavras de um

dicionário e comparações com os arquivos de senhas dos usuários. Assim, quando uma palavra do dicionário cifrada coincide com a senha cifrada de um usuário, ocorre a obtenção da senha.

DMZ: Do inglês ***D**e**M**ilitarized **Z**one*, ou "zona desmilitarizada", em português. Também conhecida como **Rede de Perímetro**, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet.

Drive-by-Download: É o *download* de um *malware* que explora a vulnerabilidade de um navegador *Web*, de um programa de *e-mail* ou de um *plug-in* de navegador, sem qualquer intervenção do usuário. O *download drive-by* pode acontecer ao se visitar um *site*, ler uma mensagem de *e-mail* ou clicar em uma janela *pop-up* enganosa.

Dump: Um despejo de banco de dados, ou *database dump*, contém um registro da estrutura de tabela e/ou dados de um banco de dados e normalmente está na forma de uma lista de declarações SQL. Um *dump* de banco de dados é muito usado para a realização de cópia de segurança de um banco de dados, desta forma seus conteúdos podem ser rearmazenados em caso de perda de dados. Bancos de dados corrompidos podem ser frequentemente recuperados pela análise do *dump*.

Esteganografia: Do grego "escrita escondida". É o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma de segurança por obscurantismo ou obscuridade. Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido. É importante frisar a diferença entre criptografia e esteganografia. Enquanto a primeira oculta o significado da mensagem, a segunda oculta a existência da mensagem.

Exploit: Exploração de vulnerabilidade. Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador. Ver também **vulnerabilidade**.

Fidonet: Uma rede de troca de mensagens entre BBS, fundada em 1984 por Tom Jennings, de São Francisco, Califórnia, Estados Unidos. O serviço era chamado *Netmail* e foi o precursor do *e-mail*

da Internet.

Firewall: Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

Flood icmp_echo: Técnica consistente em inundar o *host* alvo com requisições icmp, tornando-o comumente indisponível.

Flood smtp: Técnica consistente em lotar a caixa de entrada de um endereço *e-mail* específico.

FTP: Do inglês ***F****ile* ***T****ransfer* ***P****rotocol*. É um protocolo usado para transferir arquivos através de redes TCP/IP e também através da Internet. Apesar de ser relativamente novo (o padrão foi estabelecido apenas em 1985, ao contrário do TCP/IP e do HTTP, que foram criados durante a década de 1970), o *FTP* se tornou extremamente popular, pois é fácil de usar, seguro e oferece uma grande gama de recursos.

GPSs: Do inglês ***G****lobal* ***P****ositioning* ***S****ystem*. Sistema de posicionamento global, é um conjunto de sistemas e satélites e dispositivos que tem como função basilar fornecer informações sobre o posicionamento individual no globo terrestre. Sistema de navegação por satélite por meio de um aparelho móvel que remete dados sobre a posição de algo.

Honeypot: Pote de mel. Uma espécie de armadilha, que consiste em colocar na rede um servidor aparentemente desprotegido, com a intenção de atrair *hackers*, ou *script kids* que invadem sistemas. As informações coletadas podem ser usadas para corrigir as brechas de segurança exploradas por eles, ou mesmo identificar os invasores.

HTML: Do inglês ***H****yper****T****ext* ***M****arkup* ***L****anguage*. Linguagem universal utilizada na elaboração de páginas na Internet.

IDS: Do inglês ***I****ntrusion* ***D****etection* ***S****ystem*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

Jailbreak: É um processo que permite que aparelhos executem aplicativos não autorizados pelos fabricantes. Um aparelho com *Jailbreak* é capaz de baixar aplicativos anteriormente indisponíveis

via instaladores não oficiais, assim como aplicações adquiridas de forma ilegal. O uso de técnicas *Jailbreak* não é recomendado pelos fabricantes, já que permite a execução de aplicativos que provêm de outros lugares.

Joiners: Utilitário utilizado para unir um *software* a outro. Tem a capacidade de unir diversos arquivos em um único arquivo. Muito utilizado para anexo de *trojans* e códigos maliciosos.

Keylogger: Tipo específico de *spyware*. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*. Ver também **Sypware**.

LFI: Do inglês ***L**ocal **F**ile **I**nclusion*. Vulnerabilidade que permite o acesso pelo atacante a arquivos do servidor como senhas e até mesmo código fonte de páginas e sistemas. Comumente ocorre pela manipulação de parâmetros nas variáveis transmitidas pelos *sites*.

LogMein: É uma suíte de *software* que fornece acesso remoto a computadores através da Internet. As diversas versões foram projetadas para usuários finais e para os profissionais de suporte técnico.

Malware: Do inglês ***Mal**icious Soft**ware***. Código malicioso. Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

Man in the middle: Homem no meio, em referência ao atacante que intercepta os dados. É uma forma de ataque em que os dados trocados entre duas partes, por exemplo, você e o seu banco, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas se apercebam.

Metasploit: É um projeto de segurança de informação com o objetivo de análise de vulnerabilidades de segurança e facilitar testes de penetração (*pentests*) e no desenvolvimento de assinaturas para sistemas de detecção de intrusos.

Nmap: É um *software* livre que realiza *portscan* desenvolvido pelo Gordon Lyon, autoproclamado *hacker "Fyodor"*. É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

On time password: Senha descartável. É uma senha que perde a validade após um processo de autenticação para impedir um *phishing* da senha.

Ownar: Fracassar, humilhar. O termo é usado para expressar dominância em um sentido negativo, declarando melhores habilidades que o oponente no jogo. Em informática, significa tornar-se o proprietário de um sistema ou equipamento informático.

Packers: Sistema utilizado para comprimir ou encriptar o conteúdo de arquivos e *softwares*. Usado comumente em *malwares* e códigos maliciosos para impedir que sejam detectados por soluções antivírus e *scanners*.

Password guessing: Técnica usada por atacantes envolvendo adivinhação das senhas para acesso a recursos, contas ou ativos informáticos. Comumente é executada por meio de sistemas computacionais e grande lista de palavras para testar um grande número de senhas.

Payload: Na computação, refere-se à carga de uma transmissão de dados. É uma atividade mal-intencionada exercida pelo *malware*. O *payload* é uma ação separada da instalação e da propagação que o *malware* realiza. É o objetivo fundamental da transmissão das informações. Em segurança da informação, o *payload* pode ser modificado e carregar informações que executam ações mal-intencionadas.

Pentest: Teste de penetração. É um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa. O processo envolve uma análise nas atividades do sistema, que envolvem a busca de alguma vulnerabilidade em potencial que possa ser resultado de uma má configuração do sistema, falhas em *hardwares/softwares* desconhecidas, deficiência no sistema operacional ou técnicas contramedidas. Todas as análises submetidas pelos testes escolhidos são apresentadas no sistema, junto com uma avaliação do seu impacto e muitas

vezes com uma proposta de resolução ou de uma solução técnica.

Phishing scam: Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Pingflood: É um ataque de negação de serviço simples no qual o atacante sobrecarrega o sistema vítima com pacotes *ICMP Echo Request* (pacotes *ping*). Este ataque apenas é bem-sucedido se o atacante possui mais largura de banda que a vítima. Como a vítima tentará responder aos pedidos, irá consumir a sua largura de banda, impossibilitando-a responder a pedidos de outros utilizadores.

Port scan: *Scanner* de porta. É um aplicativo com o objetivo de testar as portas lógicas de determinado *host* remoto. Neste teste, ele identifica o *status* das portas, se estão fechadas, escutando ou abertas. Pode-se explicitar o *range* de portas que o aplicativo irá escanear, por exemplo: 25 a 80. Geralmente os *port scanners* são usados por pessoas mal-intencionadas para identificar portas abertas e planejar invasões. Podem também ser usados por empresas de segurança para análise de vulnerabilidades (*pentest*). Um dos *port scanners* mais conhecidos é o *nmap*.

ProRat: É um *backdoor* da classe Rat, que possui muitas funções de espião.

Proxy: Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar o desempenho de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. Quando mal configurado (*proxy* aberto), pode ser abusado por atacantes e utilizado para tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Satan: *Software* de auditoria e testes que coleta uma variedade de informações sobre uma rede. Ferramenta usada por administradores para avaliar a segurança de sistema e *sites*.

Screenlogger: Tipo específico de *spyware*. Programa similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites*

de *Internet Banking*. Ver também ***Spyware***.

Shells: Em sistemas derivados do Unix, o *Shell* é o componente do sistema que fornece a interface em modo texto, convertendo os comandos dados pelo usuário nas instruções entendidas pelo *kernel* do sistema. Ainda, pode significar *sites* com vulnerabilidades em suas variáveis, permitindo a injeção de código.

SIEM: Do inglês ***S**ecurity **I**nformation and **E**vent **M**anagement*. Uma abordagem de gestão em segurança da informação que visa proporcionar uma visão holística da segurança em uma empresa. O sistema coleta dados sobre a segurança em vários locais e é capaz de olhar para todos os dados em um único ponto, facilitando detectar padrões fora do comum.

SLA: Do inglês ***S**ervice **L**evel **A**greement*. É um tipo de contrato que estipula os termos de uso dos *softwares* ou equipamentos comprados ou alugados, limitações do suporte técnico, garantias de desempenho ou estabilidade, garantia de disponibilidade, dentre outros.

Slave: Escravo. Sempre que conectamos dois HDs na mesma porta, um deverá ser configurado como *master* (mestre) e outro como *slave*. O HD configurado como *master* será o usado para dar o *boot* e receberá a letra C: dentro do Dos/Windows. O *slave* receberá uma das letras sequenciais, D:, E: etc.

SmartCard: Dispositivo do tamanho de um cartão de crédito com um microprocessador embutido e uma pequena quantidade de armazenamento que é usado, com um código de acesso, para permitir autenticação baseada em certificado. *SmartCards* armazenam com segurança certificados, chaves públicas e chaves privadas, senhas e outros tipos de informações pessoais.

Sniffing: Interceptação de tráfego. Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Spyware: Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e *adware* são alguns tipos específicos de *spyware*.

SQL: Do inglês ***S**tructured **Q**uery **L**anguage*. Linguagem desenvolvida pela IBM que usa comandos

simples, baseados em palavras em inglês, para realizar buscas em bancos de dados. É suportado por várias plataformas de bancos de dados, permitindo que bancos de dados sejam criados em várias plataformas diferentes.

SQL injection: É um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQL ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (*query*) através da manipulação das entradas de dados de uma aplicação.

Sqlmap: É uma ferramenta *open source* para teste de penetração que automatiza o processo de detecção e exploração de vulnerabilidades a Injeção de SQL.

SYN flood: É uma forma de ataque de negação de serviço (também conhecido como *Denial of Service* – DoS) em sistemas computadorizados, na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

Tablets: Dispositivo pessoal em formato de prancheta que pode ser usado para acesso à Internet, organização pessoal, visualização de fotos, vídeo, leitura de livros e entretenimento.

Tcpdump: É uma ferramenta utilizada para monitorar os pacotes trafegados numa rede de computadores. Ela mostra os cabeçalhos dos pacotes que passam pela interface de rede.

Team Viewer: Tradicional programa para acesso remoto. Um programa que permite acessar uma máquina à distância.

Token: Uma estrutura de dados que contém informações de autorização para um usuário ou grupo. Um sistema usa um *token* de acesso para controlar o acesso a objetos protegíveis e para controlar a capacidade de um usuário executar várias operações relacionadas a sistema no computador local.

Trojan: Em computação, o cavalo de troia é um tipo de *malware* (código malicioso) não autorreplicante (ao contrário do *worm*) que, quando executado, normalmente realiza ações como roubo de dados e danos aos sistemas.

VNC: Do inglês ***V**irtual **N**etwork **C**omputing*. É um protocolo desenhado para possibilitar interfaces gráficas remotas. Através deste protocolo um usuário pode conectar-se a um computador remotamente, e utilizar as suas funcionalidades visuais como se estivesse sentado em frente do computador.

VPN: Do inglês ***V**irtual **P**rivate **N**etwork*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade: Condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidade são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Wireshark: Anteriormente conhecido como *Ethereal,* é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do *Wireshark* são parecidas com o *tcpdump,* mas com uma interface GUI, com mais informação e com a possibilidade da utilização de filtros.

ZERO DAY ou **0Day**: São falhas em produtos e *softwares* cujas empresas proprietárias não tiveram tempo de se proteger ou lançar a correção de segurança. Também designada uma vulnerabilidade que já está sendo explorada antes mesmo que uma correção esteja disponível. Dia zero é qualquer tempo antes que a solução da falha esteja disponível.

1 Disponível em: <http://www.quemdisse.com.br/frase.asp?frase=98851>.

2 Disponível em: <http://computerworld.uol.com.br/telecom/2013/07/12/brasil-ultrapassa-100-milhoes-de-pessoas-com-acesso-a-internet/>.

3 Discurso usado no Substitutivo oferecido em plenário em substituição à Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 2.126/2011, que estabelece princípios, garantias e deveres para o uso da Internet no Brasil. Disponível em: <http://www.camara.gov.br/internet/agencia/pdf/mci_2014_02_12_relatorio.doc>.

4 Do latim *lex talionis,* consiste na rigorosa reciprocidade entre o crime e a pena, que também denomina-se “retaliação”.

5 Disponível em: <http://pt.wikipedia.org/wiki/Joseph-Marie_Jacquard>.

6 Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.

7 Disponível em: <http://www1.folha.uol.com.br/fsp/cotidian/ff05089912.htm>.

8 Disponível em: <http://www.terra.com.br/informatica/especial/estiloweb/991214.htm>.

9 Disponível em: <www.jfrn.gov.br/institucional/biblioteca/doutrina/doutrina84.doc>.

10 Confira alguns crimes virtuais que viraram notícia. *Folha de S.Paulo*, 7-1-2006. Disponível em: <www1.folha.uol.com.br/folha/informatica/ult124u19460.shtml>.

11 Disponível em: <http://info.abril.com.br/noticias/seguranca/brasil-e-o-4-pais-com-maior-numero-de-ameacas-virtuais-04052012-16.shl>.

12 Disponível em: <http://info.abril.com.br/aberto/infonews/092004/13092004-13.shl>.

13 Disponível em: <http://agenciabrasil.ebc.com.br/noticia/2004-09-13/pesquisas-apontam-que-brasil-esta-na-rota-dos-crimes-na-internet>.

14 Disponível em: <http://g1.globo.com/Noticias/Rio/0,,MUL487856-5606,00-CRIMES+VIRTUAIS+GERAM+MAIS+DINHEIRO+DO+QUE+O+NARCOTRAFICO+DIZ+PF.html>.

15 Disponível em: <http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/09/20/crimes-ciberneticos-atingem-77-mil-brasileiros-diariamente-prejuizo-e-de-r-104-bilhoes.jhtm>.

16 Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/10/crime-cibernetico-gera-prejuizos-de-quase-r-16-bilhoes-no-brasil.html>.

17 Disponível em: <http://www.algartecnologia.com.br/portugues/noticias/em-noticia/mercado/brasil-tem-prejuizo-de-r-40-bilhoes-com-crime-cibernetico/>.

18 Disponível em: <http://www.conjur.com.br/2012-mar-02/fbi-convoca-especialistas-seguranca-guerra-cibernetica>.

19 Disponível em: <http://www.stf.gov.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=HC.SCLA.%20E%2088905.NUME.&base=baseAcordaos>.

20 Disponível em: <http://www.sertaniananet.com.br/noticiasmais/destaque/brasil-e-o-segundo-pais-com-maior-numero-de-crimes-ciberneticos>.

21 Disponível em: <http://cio.com.br/noticias/2013/07/16/governo-investe-metade-do-orcamento-de-seguranca-cibernetica-em-2012/>.

22 Disponível em: <http://seumicroseguro.com/2013/06/23/brasil-e-o-4o-principal-alvo-dos-crackers-em-ataques-phishing-no-mundo/>.

23 Disponível em: <http://olhardigital.uol.com.br/negocios/digital_news/noticias/ataques-de-phishing-atingem-38-milhoes-de-usuarios,-diz-kaspersky>.

24 Disponível em: <http://olhardigital.uol.com.br/negocios/digital_news/noticias/ataques-de-phishing-atingem-38-milhoes-de-usuarios,-diz-kaspersky>.

25 Disponível em: <http://www1.folha.uol.com.br/mercado/2014/06/1467110-brasil-perde-ate-us-8-bilhoes-com-crime-cibernetico.shtml>.

26 Disponível em: <http://brasileconomico.ig.com.br/tecnologia/2014-06-09/crimes-de-informatica-custam-cerca-us-500-bi-para-economia-mundial.html>.

27 A ferramenta HTTP Everywhere pode minimizar a incidência de *sniffers*. Disponível em: <https://www.eff.org/https-everywhere>.

28 Já se decidiu que o compartilhamento de sinal de Internet não é crime no Brasil. Disponível em: <http://portal.trf1.jus.br/portaltrf1/comunicacao-social/imprensa/noticias/turma-entende-que-compartilhamento-de-sinal-de-internet-nao-e-crime.htm>.

29 Estamos falando do modelo OSI, que é um modelo de referência com o objetivo de ser um padrão para protocolos de comunicação nos mais diversos sistemas. Mais informações em: <http://pt.wikipedia.org/wiki/Modelo_OSI>.

30 Tramita no Senado um Projeto de Lei (n. 283/2012) que atualizaria o Código de Defesa do Consumidor para vedar o envio de mensagem não solicitada.

31 Neste ponto, releva assinalar trecho de importante relatório do então Ministro do STF, Sepúlveda Pertence, no julgamento do *Habeas Corpus* 76.689/PB, de 22-9-1998, envolvendo crime cibernético: "Não se trata no caso, pois, de lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminadora, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou a redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo".

32 Disponível em: <http://www.istoedinheiro.com.br/noticias/99920_EMPRESAS+GASTAM+6+MAIS+COM+CRIMES+VIRTUAIS+EM+2012>.

33 Lista dos países signatários disponível em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG>.

34 O Relatório da Convenção de Budapeste pode ser acessado em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf>.

35 O texto em português da Convenção pode ser acessado em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.

36 Embora tenhamos casos considerados de alta tecnologia, como o vírus STUXNET, programa malicioso que atacou diversos sistemas de controle industrial da marca Siemens (SCADA), utilizados por muitas indústrias, inclusive nucleares. Saiba mais em: <http://www.tecmundo.com.br/virus/5878-stuxnet-o-virus-da-pesada.htm>.

37 A respeito, citem-se importantes artigos científicos e livros sobre o tema, como:

a) "Criminal profiling and insider cyber crime", escrito por Nick Nykodym, Robert Taylor, Julia Vilela, da Universidade de Toledo, Ohio-USA, que buscaram em suas pesquisas detectar características que aparecem regularmente em crimes cibernéticos, apontando a utilidade para empresas na detecção proativa de cibercriminosos;

b) "The role of criminal profiling in the computer forensics processes", escrito por Marc Rogers, onde o autor aborta a importância de se conhecer o perfil do criminoso digital no processo de computação forense;

c) "The role of behavioral research and profiling in malicious cyber insider investigations", escrito por Eric D. Shaw, que faz um minucioso estudo sobre o perfil dos ataques internos;

d) *Profiling Hackers*: The Science of Criminal Profiling as Applied to the World of Hacking, livro escrito por Raoul Chiesa, Stefania Ducci, Silvio Ciappi, que também tenta estabelecer um perfil dos atacantes digitais.

38 Um compilado sobre disposições acerca do cibercrime nos Estados Unidos pode ser acessado em:

<http://www.oas.org/juridico/spanish/us_cyb_laws.pdf>.

39 Acesso à legislação em: <http://www.senate.gov.ph/lisdata/111349486!.pdf>.

40 Disponível em: <http://www.gesetze-im-internet.de/stgb/index.html>.

41 Íntegra da legislação em: <http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4E472CDE49F1945CFD9516C29A2B1B21.tpdila09v_1?cidTexte=JORFTEXT000000801164&dateTexte=20150623>.

42 Legislação acessível em: <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

43 Código Penal da Espanha – disponível em: <http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20121008_02.pdf>.

44 Acesso à legislação argentina em: <http://www.protecciondedatos.com.ar/ley25326.htm>.

45 Disponível em: <http://www.portaldoconsumidor.gov.br/noticia.asp?id=27245>.

46 Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/hackers-atacam-sites-da-presidencia-do-governo-brasileiro-2759562.

47 Disponível em: <http://www.linhadefensiva.org/wp-content/uploads/2012/05/pl84-99-senado.pdf>. Este substitutivo foi novamente revisto na Câmara dos Deputados, sendo que, ao final, em acordo entre deputados, diversos artigos foram suprimidos e um texto básico proposto para votação, que resultou na aprovação da Lei n. 12.737/2012.

48 Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Msg/VEP-525.htm>.

49 O documento pode ser acessado em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1034065&filename=Avulso+-PL+84/1999>.

50 Disponível em: <http://legis.senado.leg.br/mateweb/arquivos/mate-pdf/13674.pdf>.

51 Em <http://www.camara.gov.br/proposicoesWeb/prop_pareceres_substitutivos_votos;jsessionid=E3913D8A28923016E5EA45B2297B8153.no idProposicao=15028> é possível verificar todas as versões do Projeto de Lei, da versão inicial até a que chegou em seu estágio resumido, disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1037657&filename=RDF+1+%3D%3E+PL+84/1999>.

52 Para saber mais, consulte: <http://culturadigital.br/dadospessoais/>.

53 A lei está disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm#art2>.

54 O STJ, atualmente, fixou entendimento de que os provedores devem guardar *logs* por 3 (três) anos. Já o Marco Civil da Internet prevê a obrigatoriedade de guarda por 6 (seis) meses para provedores de aplicações e 1 (um) ano para provedores de acesso.

55 Disponível em: <http://www.teletime.com.br/04/10/2012/perdas-com-cibercrimes-chegam-a-r-15-bilhoes-no-brasil-por-ano/tt/304178/news.aspx>.

56 A energia elétrica é passível de furto no Brasil. No julgamento do Recurso em Sentido Estrito 70057761058, o Tribunal de Justiça do Rio Grande do Sul entendeu que, inexistindo perícia técnica, é de se manter a decisão que rejeitou a denúncia por furto de energia elétrica (publicado em 24-1-2014).

57 Nesse sentido, notícia “Copiar arquivos digitais sem autorização do empregador não é furto, decide TJRS”. Disponível em: <http://www.conjur.com.br/2014-mai-26/copiar-arquivos-digitais-autorizacao-nao-furto-decide-tj-rs>.

58 Disponível em: <http://www.btadvogados.com.br/pt-br/content/crime-de-perigo-abstrato>.

59 Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>.

60 No Código Penal, por exemplo, o agente que copiasse informação, enquadrando-se no crime de furto, responderia por uma pena maior do que o agente que destruísse a informação, onde forçosamente deveria ser enquadrado no delito de dano, previsto no art. 163. Estas falhas foram supridas com a Lei n. 12.737/2012.

61 Disponível em: <http://g1.globo.com/economia/noticia/2012/04/brasil-ultrapassa-em-marco-marca-de-250-milhoes-de-celulares-diz-anatel.html>.

62 Projeto de Lei n. 89/2003.

63 *Ransonware* é caracterizado pelo sequestro de ativos informáticos onde se exige resgate para a devolução. Atualmente, ferramentas criptografam dados, onde a liberação dos mesmos só será possível mediante pagamento. Saiba mais em: <http://itweb.com.br/blogs/sequestro-digital-por-que-algo-tao-antigo-continua-tao-recente/>.

64 Disponível em: <http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/08/google-remove-app-rastreador-de-namorado-de-sua-loja-pela-2-vez.html>.

65 Nesse sentido, dispõe o art. 3º da Lei n. 109/91 que “as pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo e pelos seus órgãos ou representantes”.

66 Disponível em: <http://olhardigital.uol.com.br/noticia/75_das_grandes_empresas_no_brasil_ja_usam_cloud_computing_aponta_estudo/18602>.

67 MAC (*Media Access Control*) Address, também conhecido como endereço físico, é o endereço da interface de rede de um computador. Ele é único e não existem no mundo dois endereços MAC iguais. Ao clonar um endereço MAC, um agente consegue ter acesso a uma rede controlada ou mesmo a recursos computacionais aos quais não teria direito.

68 Disponível em: <http://g1.globo.com/distrito-federal/noticia/2013/09/compartilhamento-de-sinal-de-internet-nao-e-crime-decide-justica.html>.

69 Os crimes de telecomunicações estão elencados na Lei Geral de Telecomunicações, n. 9.472/92.

70 Ver Lei n. 8.935/94, disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8935.htm>.

71 Importante mencionar que nos Estados Unidos a interpretação do Electronic Communications Privacy Act (ECPA), no que tange ao uso de Internet Wireless, vem sendo que se o titular da Internet mantém o tráfego não criptografado ou a rede não oculta, caso ele venha a ser interceptado, não há que se falar em violação ou crime. Mais, se mantinha uma criptografia fraca (WEP), mesmo sendo um mecanismo já superado, fica a vítima protegida pela legislação norte-americana.

72 Nesse sentido, a exemplo, verifica-se recente conflito de competência em processo n. 1.219.125-6, apreciado pelo Tribunal de Justiça do Paraná, onde o Juiz de Direito do 11º Juizado Especial suscitou conflito negativo de competência, em processo de pedido de quebra de sigilo de dados por suposta violação ao art. 154-A do Código Penal, por tratar de feito onde não se tem conhecimento do autor do crime e

entendeu o juiz não ser apropriado para seguir os trâmites dos Juizados Especiais Criminais, uma vez que poderia ser necessária a produção de provas, perícias etc. Nesse vértice, suscitou o conflito negativo de competência com fundamento no art. 77, §§ 1º e 2º, e no art. 66, parágrafo único, da Lei n. 9.099/95. Inteiro teor em: <http://tj-pr.jusbrasil.com.br/jurisprudencia/150359978/conflito-de-jurisdicao-cj-12191256-pr-1219125-6-acordao/inteiro-teor-150359984>.

73 Uma das principais ferramentas utilizadas para realização do DDoS é o LOIC (*Low Orbit lon Cannon*), um programa de computador de código aberto escrito em C#, que tem como objetivo a execução de ataques de negação de serviço, desenvolvido pela Praetox Technologies em 2006 com o escopo de avaliar e testar as redes, tendo sido posteriormente disponibilizado para domínio público.

74 Detalhes sobre o SynFlood podem ser obtidos em: <http://pt.wikipedia.org/wiki/SYN_Flood>.

75 A utilização de programas como WireShark e Cain, conquanto não interrompessem os serviços telemáticos, poderia ser enquadrada no conceito de "perturbação", daí por que o legislador penal se preocupar apenas com a interrupção de serviços telemáticos.

76 Disponível em: <http://www.terra.com.br/informatica/2002/07/10/001.htm>.

77 Disponível em: <http://cbn.globoradio.globo.com/editorias/tecnologia/2012/08/04/PHISHING-CRESCE-89-NO-BRASIL-NO-SEGUNDO-TRIMESTRE-DE-2012.htm>.

78 Disponível em: <http://www.correiobraziliense.com.br/app/noticia/tecnologia/2013/11/19/interna_tecnologia,399263/brasil-e-o-quarto-pais-com-vitimas-de-crimes-virtuais-segundo-afcc.shtml>.

79 AgRg no CComp 110.855/DF, rel. Min. Og Fernandes, 3ª Seção, julgado em 13-6-2012, *DJe* de 22-6-2012. Inteiro teor: <http://br.vlex.com/vid/-382163414>.

80 CComp 101.900/RS, rel. Min. Jorge Mussi, 3ª Seção, julgado em 25-8-2010, *DJe* de 6-9-2010. Inteiro teor: <http://www.radaroficial.com.br/d/7670970>.

81 No sentido de que o fato, nessas hipóteses, é atípico: Cézar Roberto Bitencourt, *Lições de direito penal*, Porto Alegre, Livr. do Advogado, 1995, p. 40; STJ, RHC 4.311, 6ª Turma, rel. Min. Vicente Cernicchiaro, *DJU* de 19-6-1995, p. 18751; STJ, REsp 112.600, 6ª Turma, rel. Min. Vicente Cernicchiaro, *DJU* de 17-8-1998, p. 96.

82 Disponível em: <http://www.opposingviews.com/i/politics/dubious-proposal-amending-computer-fraud-and-abuse-act#>.

83 Disponível em: <http://www.fecomercio.com.br/NoticiaArtigo/Artigo/3834 1>.

84 Acessível em: <http://www.honeyd.org/>.

85 Acessível em: <http://www.honeynet.org.br/>.

86 Disponível em: <http://www.information-age.com/technology/security/2133923/use-honeypots-to-catch-cyber-criminals-says-enisa>.

87 Precedentes: HC 38.758, HC 40.289, RE 15.531, RHC 27.566.

88 Disponível em: <http://veja.abril.com.br/081106/p_134.html>.

89 Um exemplo de infecção *Drive-by-Download* que infectou milhares de usuários no Brasil pode ser acessado em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1300037-6174,

00-MAIS+DE+MIL+INTERNAUTAS+PODEM+TER+SIDO+INFECTADOS+POR+SITE+DA+VIVO.html>.

90 A versão em português pode ser encontrada em: <http://owasptop10.googlecode.com/files/OWASP_Top_10_-_2013_Brazilian_Portuguese.pdf>.

91 Embora não seja objeto deste capítulo, importante mencionar que programas conhecidos como *crawlers* podem fazer o *download* de páginas *web* de um servidor (linkadas). Ainda, alguns programas podem indicar o nome dos arquivos existentes em um FTP. Não há que se falar em invasão nestes casos, considerando que não existe rompimento de obstáculo algum para acesso aos arquivos ou nomes dos arquivos.

92 O texto em português pode ser obtido em: <http://www.acidi.gov.pt/_cfn/529350b642306/live/+Conven%C3%A7%C3%A3o+sobre+o+Cibercrime++>.

93 Acesso ao relatório em: <http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf>. Versão 2015 disponível em: <https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf>.

94 Relatório com as senhas mais utilizadas no mundo pode ser encontrado em: <https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf>, p. 104.

95 A consulta era disponibilizada no *site*: <http://culturadigital.br/marcocivil>.

96 Para acessar o texto do Marco Civil: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=918144&filename=Avulso+-PL+2126/2011>.

97 Disponível em: <http://www.cg.org.br/publicacoes/documentacao/desenvolvimento.htm>.

98 Nesse sentido "Gráfico para apuração judicial de crimes digitais", desenvolvido por José Antonio Milagre, pode ser obtido em: <http://josemilagre.com.br/blog/sala-de-estudos/direito-tecnologico/documentos/grafico-para-apuracao-judicial-de-crimes-digitais/>.

99 Como exemplo, o Estado de São Paulo, com a Lei n. 12.228/2006. Disponível em: <http://www.crianca.mppr.mp.br/arquivos/File/legis/lei_estadual_12228_2006_sp.pdf>.

100 A respeito, consultar livro dos autores sobre o Marco Civil da Internet: *Marco Civil da Internet*: comentários à Lei n. 12.965/14. São Paulo: Saraiva, 2014.

101 Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=150517&tp=1>.

Também está em trâmite no Brasil o Projeto de Lei n. 494/2008, que aumenta o prazo para que os provedores de Internet e empresas de telecomunicações mantenham a guarda dos *logs*. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/88862>.

Igualmente em trâmite o Projeto de Lei n. 215/2015, que torna ainda mais abrangente a retenção de dados e trata do direito ao esquecimento, tendo sido aprovado na Comissão de Constituição e Justiça da Câmara em 6-10-2015. Disponível em: <http://www2.camara.leg.br/camaranoticias/noticias/DIREITO-E-JUSTICA/493762-PROJETO-AUMENTA-PENA-PARA-CRIME-CONTRA-HONRA-COMETIDO-EM-REDES-SOCIAIS.html>.

102 Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>.

103 TRF, HC 33.200/SP (2010.03.00.0033200-0). Inteiro teor disponível em: <http://tnu.jusbrasil.com.br/jurisprudencia/20606584/hc-habeas-corpus-hc-201103000101390>.

104 Em recente decisão nos Estados Unidos (*Circuit Court*) um juiz entendeu que um usuário deve fornecer suas impressões digitais para um policial acessar seu dispositivo móvel, mas não é obrigado a fornecer sua senha. Mais detalhes em: <http://hamptonroads.com/2014/10/police-can-require-cellphone-fingerprint-not-pass-code>.

105 TRF, 4ª Região, AC 2002.04.01.029123-1/PR, Rel. Fábio Rosa, 7ª Turma, unânime, *DJ* de 21-5-2003.

106 O *e-mail* de contato é cybercrime_brazil_24x7@dpf.gov.br.

107 O *e-mail* de contato é cooperacaopenal@mj.gov.br.

108 Existe MLAT entre Brasil e Estados Unidos. Acesse: <http://ascji.pgr.mpf.gov.br/informes-e-documentos/documentos/brazil_MLAT.ppt/view>.

109 No *site* do Ministério da Justiça é possível conhecer as regras de cooperação internacional de vários países, legislação interna, instrumentos de cooperação e outros detalhes. Recomenda-se a leitura antes da formulação de um pedido. Disponível em: <http://portal.mj.gov.br/data/Pages/MJE1AEA228PTBRIE.htm>.

110 Uma lei americana muito divulgada no Brasil pelos provedores de serviços, com escopo de não se submeterem às ordens locais, é o

Electronic Communications Privacy Act de 1986.

111 Para pessoa estrangeira com sede no Brasil, vale a regra do art. 12 do Código de Processo Civil, que assim dispõe: “Art. 12. Serão representados em juízo, ativa e passivamente: (...) VIII – a pessoa jurídica estrangeira, pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil (art. 88, parágrafo único)”.

112 Recomenda-se conhecer o FIRST, uma rede global de *times* de resposta a incidentes de segurança. Disponível em: <http://www.first.org/>.

113 Os endereços das delegacias podem ser acessados em: <http://www.safernet.org.br/site/prevencao/orientacao/delegacias>.

114 Disponível em: <http://www.senado.gov.br/atividade/materia/getTexto.asp?t=158984&c=PDF&tp=1>.

115 Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=106404>. Em 8-6-2015, o projeto foi enviado para a Comissão de Justiça e Cidadania no Senado.

116 Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=619448>.

117 Disponível em: <http://jus.com.br/revista/texto/4992/da-validade-juridica-dos-contratos-eletronicos#ixzz2ZeWGk7M7>.